数 の 世 界

数 の 世 界

――整数論への道――

和 田 秀 男 著

岩 波 書 店

まえがき

この本の第1の目的は，初等整数論の面白さを高校生にもわかるように伝えることである．第2の目的は“素数を表わす多項式”について，何の予備知識が無くともわかるように説明することである．数学を勉強するうえで一番大切なことは，数学と親しみ，数学を楽しむことである．幸い整数論においては，小学生のころから計算を行ない，約数や倍数について学んでいる．よって具体的に計算することはだれにでも可能であり，少しの説明で数を楽しむことが出来る．本書は読者が具体的な計算をどしどし行なえるように，計算法を大切にし，計算の手順をはっきりさせるように努めた．読者は出来うるかぎり筆算やソロバン，電卓などを利用して計算を実行してほしい．具体的に苦労して計算することによって，本当の面白さがわかってくると思う．

前編は第1の目的のために書いた．できるだけやさしく，しかも具体的な例を多く示すように努めた．第1章は，パズル的な計算より自然数そのものに親しんでもらおうと思って書いた．また合同式の考え方や，ディリクレの部屋割り論法に慣れてもらうようにした．第2章は，最大公約数を求めるとき，ユークリッドの互除法がいかに強力な計算法であるかを示した．また互除法の副産物として，1次不定方程式が具体的に解けることを示した．第3章は，どのような自然数も，素数の積としてただ1通りに表わせる，という初等整数論の基本定理を互除法を使って示した．直接に，巧妙にこの基本定理を証明することも出来るけれど，具体的な計算法を大切にする立場に立ち，互除法からの流れを利用した．第4章は，約数と倍数についてであるが，基本定理を使うと多くのことをすっきり説明す

ることが出来る．ただし具体的に計算するときは，互除法以上に優れた方法はない．§7の後半に積分を利用するが，この結果は§8にのみ利用するので，積分を学んでいない読者は§7の後半と§8は飛ばして差し支えない．第5章は，合同式についてである．2つの自然数があったとき，割り切れるか否か，割り切れなければ余りがいくつになるか，などを含んだどのように複雑な問題も，合同式を利用すると非常に見通しよくなる．§6において，どのような自然数も4つ以下の平方数の和になる，というラグランジュの定理の証明を加えた．面白い定理だと思う．第6章において，まずフェルマーの定理を証明した．この定理は，初等整数論においてたえず有効に利用されるものである．特別の利用法として，素数か否かの判定に使われる．このとき，a^n を計算しなければならないが，2進法を使うと互除法と同じように能率的に計算出来る．さて，複素数の1の n 乗根に対応するものが原始根である．原始根を利用すると，4で割ると1余るどのような素数も2つの平方数の和になることが証明出来る．美しい定理だと思う．

後編は2次式の整数論である．前編は主に1次式についての整数論であるから，後編は一段とむずかしくなる．高校生には少し無理かも知れないが，それは証明が長くなるからであって，予備知識は特に必要ではないから忍耐力さえあれば読み終えることが出来ると思う．第7章は，相互律についてである．この相互律は整数論をパズル的な世界から学問の世界へと高めるものである．相互律の意味するものは深遠である．ただただガウスの天才に頭を下げるのみである．第8章は，ペル方程式についてである．双曲線 $x^2-my^2=1$ の上に，x 座標も y 座標も整数である点が無限にあることは，神秘的な結果だと思う．この章では，いかに x, y を具体的に計算するかを幾何学的に考え，無理がないように説明した．第9章は，或る大

きな自然数が与えられた場合，それが素数であるか否かどのように判定するか，また素数でないとわかったとき，どのように分解するか，などの具体的な方法を示した．第10章は，第2の目的である“素数を表わす多項式”についてである．19変数の多項式を具体的に作り，変数に自然数を代入したとき素数となり，しかも変数の値を変えるとすべての素数が現われることを証明した．少し専門的ではあるが，ウィルソンの定理とペル方程式が解を持つという事実以外は何も使っていないから，根気よく読めば理解出来る．

10年程前“電子計算機と初等整数論”という題で書いた雑文をまとめようと思いこの本を書きはじめた．しかし2つのことを同時に書くのは無理があるので，電子計算機については別の機会に書くことにし，本書では計算結果のみを利用することにした．初等整数論については私の大学の数学科1年生に何度か講義したので，その内容を基にして前編をまとめることにした．私の興味でもあったが後編の“素数を表わす多項式”は，その証明が初等整数論の範囲で出来ることがわかったので，つけ加えることにした．読者が少しでも面白いと感ずる部分を見つけることが出来れば幸いである．

恩師彌永昌吉先生は，私がこの本を書こうと思ったとき，岩波書店の編集部へ紹介して下さった．院生の永田清君と関口晃司君には原稿の前編と後編をそれぞれ見なおしていただいた．岩波書店では，荒井秀男氏に永い間辛抱強く原稿の出来るのを待ってもらい，いろいろお世話になった．荒井氏の忍耐力がなければこの本は出来なかったと思う．上記の方々に厚くお礼申し上げます．

昭和56年5月

和田秀男

目　次

後　　編

第7章　相互律

第8章　ペル方程式

第9章　素数判定法

前　　編

第1章　数と遊ぶ

§1　九去法

このごろは電卓が普及したので，四則計算を行なうのは容易になった．しかし計算の結果が正しいだろうか，と疑問になったとき，昔から知られている九去法という検算法は面白いし，有用なので紹介しよう．

$$
\begin{array}{r}
72702 \\
9\overline{)654321} \\
\underline{63} \\
24 \\
\underline{18} \\
63 \\
\underline{63} \\
021 \\
\underline{18} \\
3
\end{array}
$$

まず適当に大きな数，たとえば654321を9で割った余りは，割り算を実行すれば3となる．しかし割り算を実行しなくとも余りは容易に求めることが出来る．その方法は各桁の数を加えれば良いのである．すなわち

$$6+5+4+3+2+1=21$$

となり，21をさらに2桁目と1桁目に分けて加えれば $2+1=3$ となり余り3が得られる．何故これで良いのか考えてみよう．

$$
\begin{aligned}
654321 &= 6\cdot10^5+5\cdot10^4+4\cdot10^3+3\cdot10^2+2\cdot10+1 \\
&= \{6\cdot(10^5-1)+6\}+\{5\cdot(10^4-1)+5\} \\
&\quad +\{4\cdot(10^3-1)+4\}+\{3\cdot(10^2-1)+3\} \\
&\quad +\{2\cdot(10-1)+2\}+1
\end{aligned}
$$

$$= 6\cdot 99999+6+5\cdot 9999+5+4\cdot 999+4$$
$$+3\cdot 99+3+2\cdot 9+2+1$$
$$= 9\cdot(6\cdot 11111+5\cdot 1111+4\cdot 111+3\cdot 11+2)$$
$$+(6+5+4+3+2+1)$$

となり，654321 を 9 で割った余りは 21 を 9 で割った余りと等しくなる．同じ計算で

$$21 = 2\cdot 10+1 = 2\cdot(9+1)+1 = 2\cdot 9+(2+1)$$

から余りが 3 となる．これらのことから，6, 5, 4, 3, 2, 1 をどのような順に並べて作った 6 桁の数も 9 で割れば 3 余ることがわかる．各桁の合計がいつも 21 になるからである．

一般に $10^n-1=999\cdots 9=9\times 111\cdots 1$ となることに気が付けば，或る数を 9 で割った余りは各桁の数を加えたものから得られることがわかるであろう．この事実を使えば，たとえば

$$235\times 412 = 96820$$

が正しいか否か判定出来る．もし等しいならば，両辺を 9 で割った余りは等しいであろう．今まで述べてきた方法を使えば

$$2+3+5 = 10, \qquad 1+0 = 1$$
$$4+1+2 = 7$$

から左辺の第 1 項は $9m+1$ という形となり，第 2 項は $9n+7$ という形をしている．その積は

$$(9m+1)\cdot(9n+7) = 9^2\cdot mn+9\cdot(7m+n)+7$$

となり，9 で割った余りは 7 となる．右辺を 9 で割った余りは

$$9+6+8+2+0 = 25, \qquad 2+5 = 7$$

から 7 となる．よって上記の乗算は正しいであろうと判定して良い．勿論 9 で割った余りが等しくても答が間違っていることもあろう．しかしその可能性は $\dfrac{1}{9}$ に減ったわけである．

次に割り算の検算を考えよう．たとえば

$$56789123 \div 9876 = 5750 \quad \text{余り} \quad 2123$$

がもし正しいならば

$$56789123 = 9876 \times 5750 + 2123$$

となる．右辺の3つの項は

$$9+8+7+6 = 30, \qquad 3+0 = 3$$

$$5+7+5+0 = 17, \qquad 1+7 = 8$$

$$2+1+2+3 = 8$$

から $9m+3$, $9n+8$, $9l+8$ という形をしている．よって右辺を9で割ると

$$(9m+3)\cdot(9n+8)+9l+8$$

$$= 9^2\cdot mn+9\cdot(8m+3n+l)+3\cdot 8+8$$

$$3\cdot 8+8 = 32, \qquad 3+2 = 5$$

から5となることがわかる．左辺を9で割ると

$$5+6+7+8+9+1+2+3$$

$$= 5+(6+3)+(7+2)+(8+1)+9$$

から5余ることがわかる．よって上記の割り算は正しいであろうと判定出来る．

以上のように，両辺を9で割った余りが等しいか否かによって，計算が正しく行なわれたか否かが確かめられる．この方法を**九去法**という．9の倍数を捨て去った残りを考えるからである．九去法を使うと次のようなこともできる．

例　数あてゲーム

A：“或る1つの数を考えて紙に書いて下さい.”

B：Aに見えないように1226と紙に書く．

A：“その数の各桁の数字を加えて下さい.”

B：$1+2+2+6=11$ とこっそり計算する．

A：“出来た数をもとの数から引いて下さい.”

B：1226－11＝1215 と計算する．

A："出来た数の各桁の数字の順をめちゃめちゃにして下さい．"

B：1215 から 5112 を作る．

A："72 を加え，出来た数から数字を 1 つ消して下さい．"

B：5112＋72＝5184，8 を消して 514 を得る．

A："出来た数の各桁の数字の和を教えて下さい．"

B：5＋1＋4＝10 であるから"和は 10 です"と答える．

A："消した数字は 8 ですね．"

B："何故わかったのですか？"

A："教えられた数を 9 で割り，その余りを 9 から引けば良いのです．今の場合，10 を 9 で割れば，余りは 1 となるので，9－1＝8 が消した数字になります．何故かといえば数字を 1 つ消す前の値は 9 で割り切れるからです．"

§2　何曜日か

今年のカレンダーを見て来年の何月何日は何曜日だろうか，と考えることがある．1 年は 365 日であるから

$$365 = 7\times 52+1$$

から，1 年は 52 週と 1 日である．よって曜日は今年と来年では 1 日だけずれる．今年の 1 月 1 日が土曜なら来年の 1 月 1 日は日曜となる．今年の 4 月 1 日が金曜なら来年の 4 月 1 日は土曜となる．ただし来年が**うるう年**の場合は，2 月が 29 日まであるので 3 月からは 2 日ずつずれる．よって来年がうるう年ならば 4 月 1 日は日曜となる．

うるう年は何故必要なのだろうか．天文学によれば，地球が正確に太陽を 1 周するのは

365.2422 日

＝365 日 5 時間 48 分 46 秒

となっている．よって1年を365日とすると

$$0.2422\times 4 = 0.9688 \doteqdot 1$$

であるから4年に約1日ずれてくる．よってうるう年を作らねばならないことがわかる．4年に1日ずらすと，100年には25日ずれることになる．しかし実際は，

$$0.2422\times 100 = 24.22 \doteqdot 24$$

であるから，100年に25日ずらすのは，1日だけずらし過ぎである．よって100年目はうるう年にしない方が良い．つまり100年間に24日ずらすわけである．このようにすると，400年間には24×4=96日ずらすことになる．しかし実際は

$$0.2422\times 400 = 96.88 \doteqdot 97$$

であるから400年間には97日ずれてほしい．よって400年目はうるう年にした方が良い．

このようなわけで，1582年，法王グレゴリー13世は，4年に1度あるうるう年の例外として，世紀の変わり目の年で，400で割れない

1700, 1800, 1900, 2100, …

はうるう年ではなく，400で割れる

1600, 2000, 2400, 2800, …

はうるう年にしよう，というグレゴリオ暦を制定した．

このように，はっきりうるう年が定められているので，西暦y年m月d日は何曜日か，計算する公式を作ることが出来る．曜日は7を周期としているので，曜日に対応する数を

日 = 0,　月 = 1,　火 = 2,　水 = 3,　木 = 4,
金 = 5,　土 = 6

とする．この曜日に対応する数が求まれば良い．

まず通常の年は365日であり

$$365 = 7\times 52+1$$

であるから1年過ぎると曜日は1日ずれる．よってもしグレゴリオ暦が西暦0年から始まるとし，うるう年のことを考えなければ，西暦 y 年には y 日だけずれる．さて西暦 y 年までには何回うるう年があるだろうか．通常は4年に1度あるから，大雑把に数えて y を4で割った回数だけあるであろう．もう少し正確に表わすために**ガウス記号**を使おう．実数 x に対して $[x]$ は x を越えない最大の整数を意味し，ガウス記号と呼ばれている．たとえば $[5.9]=5$, $[3.0]=3$ となる．よって $[x]$ は x の整数部を意味する．この記号を使えば西暦 y 年までには

$$[y/4]-[y/100]+[y/400] \text{ 回}$$

うるう年がある．y が4つ増すと $[y/4]$ は1つ増す．つまり4年に1度のうるう年に対応する．しかし 1700, 1800, 1900, 2100 という世紀の変わり目はうるう年でないので $[y/100]$ を引く必要がある．さらに 1600, 2000, 2400, 2800 という 400 で割れる世紀の変わり目はうるう年なので $[y/400]$ を加えるわけである．結局西暦 y 年までには

$$a = y+[y/4]-[y/100]+[y/400] \text{ 日}$$

だけ曜日がずれてくる．

以上でうるう年に関する情報量 a は定まったが，次に m 月 d 日に関する情報量を求めてみよう．ここで問題なのはうるう年とは2月が1日増して29日となることなので，影響を受けるのは3月1日の曜日からであり，1月，2月は影響を受けない事実である．よって3月，4月，…を3月から数えて1番目の月，2番目の月，…と数えた方が公式を作りやすい．1月，2月は前の年の11番目の月，12番目の月と数えるわけである．つまり西暦 y 年の m 月を，

$$y' = \begin{cases} y, & 3 \leqq m \text{ のとき} \\ y-1, & m = 1,2 \text{ のとき} \end{cases}$$

$$m' = \begin{cases} m-2, & 3 \leqq m \text{ のとき} \\ m+10, & m=1,2 \text{ のとき} \end{cases}$$

とおいたとき，西暦 y' 年の m' 番目の月と数えるわけである．さて m' 番目の月の第 1 日目は 3 月 1 日とくらべてどのくらい曜日がずれているだろうか．もし $g(m')$ 日だけずれているならば，うるう年に関する情報量 a と合せて，西暦 y' 年の m' 番目の月の第 d 日の曜日が

$$w = a+g(m')+d+C \qquad (C\text{ は定数})$$

を 7 で割った余りに対応する曜日になるように定数 C を定めることが出来る．

まず，$g(m')$ のとるべき値を考えよう．3 月 1 日を基準にすれば，3 月は 31 日あるので $31=4\times7+3$ から 4 月 1 日は 3 日だけ曜日がずれる．4 月は 30 日だから 5 月 1 日は 3 月 1 日とくらべて 5 日だけ曜日がずれる．以下順に計算すると表 1-1 が出来る．

表 1-1

m	m'	$g(m')$	$g(m')-2m'$	m	m'	$g(m')$	$g(m')-2m'$
3	1	0	−2	9	7	16	2
4	2	3	−1	10	8	18	2
5	3	5	−1	11	9	21	3
6	4	8	0	12	10	23	3
7	5	10	0	1	11	26	4
8	6	13	1	2	12	29	5

$g(m')$ の増え具合は平均 $29/11 \fallingdotseq 2.64$ である．グラフに書くと勾配が約 2.64 になり，2 より少し大きい．グラフに書くためには勾配を小さくした方が見易いので，勾配を 2 だけ小さくし $g(m')-2m'$ のグラフを書くと図 1-1 のようになる．

$g(m')-2m'$ を直線 $y=kx+b$ で近似したい．またガウス記号を使

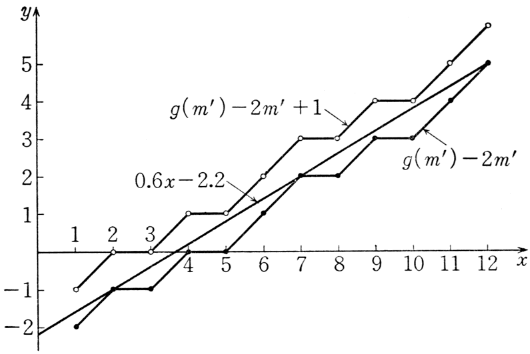


図 1-1

い$[km'+b]=g(m')-2m'$ としたい．そのためには

(1) $$g(m')-2m' \leqq km'+b < g(m')-2m'+1$$

となってほしい．定木を使っていろいろ試みると，$m'=2, 7, 12$ のとき $g(m')-2m'$ という値をとる $y=0.6x-2.2$ という直線が(1)を満たすことがわかる．よって

$$g(m') = [0.6m'-2.2]+2m'$$

となる．一般に n を整数とすれば，$x+n$ の整数部は x の整数部に n を加えたものになる．つまり $[x+n]=[x]+n$ となる．同様に $[x-n]=[x]-n$ となるので

$$\begin{aligned} g(m') &= [2.6m'-2.2] \\ &= [2.6m'-0.2]-2 \\ &= [(13m'-1)/5]-2 \end{aligned}$$

が得られる．以上をまとめると

$$\begin{aligned} w = y'+[y'/4]-[y'/100]+[y'/400] \\ +[(13m'-1)/5]-2+d+C \end{aligned}$$

となる．グレゴリオ暦は 1582 年 10 月 15 日金曜日から始まる．こ

のとき $y'=1582, m'=8, d=15$ となり，よって w を7で割った余りが5となるように定数 C を定めれば良い．

$$\begin{aligned}&1582+[1582/4]-[1582/100]+[1582/400]\\&\quad+[(13\times 8-1)/5]-2+15+C\\&\quad= 1582+395-15+3+20-2+15+C\\&\quad= 1998+C = 7\times 285+3+C\end{aligned}$$

となるので $C=2$ と定めれば良い．以上のことをまとめると

$$w=y'+[y'/4]-[y'/100]+[y'/400]+[(13m'-1)/5]+d$$

となる．

例　広島に原子爆弾が投下された1945年8月6日は何曜日か．

この場合，$y'=1945, m'=6, d=6$ であるから

$$\begin{aligned}w &= 1945+486-19+4+15+6\\&= 7\times 348+1.\end{aligned}$$

よって月曜日であった．——

例　21世紀の最初の日，2001年1月1日は何曜日か．

この場合，1月は前の年の11番目の月と数えるので $y'=2000, m'=11, d=1$ となる．よって

$$\begin{aligned}w &= 2000+500-20+5+28+1\\&= 7\times 359+1\end{aligned}$$

つまり21世紀の最初の日は月曜日である．——

以上のように曜日を求めるには7で割った余りのみが大切である．このようなとき，**7を法**として考える，という．記号では **mod 7** で考える，という．

§3　フィボナッチ数列

フィボナッチは1202年“Liber Abaci”という優れた商業算術の本を著した．その本の中に次のような問題がある．

(1) 1月1日，或る囲い地に1つがいのウサギがいた．

(2) 2月1日に1つがいのウサギを生んだ．さらにつづけて1か月ごとに1つがいのウサギを生んだ．

(3) 子ウサギは1か月で親ウサギとなり，さらに1か月たつと1つがいのウサギを生んだ．

さて，次の年の1月1日には何つがいになるだろうか．

この問題を解くために，親と子が何つがいになるか，数えてみよう．1か月過ぎるごとに親が子を生み，子は親になるから次の表1-2が作られる．

表 1-2

	親	子	総
1月1日	1	0	1
2月1日	1	1	2
3月1日	2	1	3
4月1日	3	2	5
5月1日	5	3	8
6月1日	8	5	13
7月1日	13	8	21
8月1日	21	13	34
9月1日	34	21	55
10月1日	55	34	89
11月1日	89	55	144
12月1日	144	89	233
1月1日	233	144	377
	F_{n+1}	F_n	F_{n+2}

よって答は377つがいとなる．n か月後に子が F_n つがいとなるとすると，この表から

(4) $$F_{n+2}=F_{n+1}+F_n,\qquad F_1=1,\qquad F_0=0$$

となっていることに気付く．次にこの事実を証明しよう．

n か月後に親が P_n つがいになるとすると

$$P_{n+1} = P_n + F_n, \qquad F_{n+1} = P_n$$

であるから

$$\begin{aligned} F_{n+2} &= P_{n+1} \\ &= P_n + F_n \\ &= F_{n+1} + F_n \end{aligned}$$

となるからである．

ところで，(4)により定義される数列を**フィボナッチ数列**と呼ぶ．フィボナッチ数列にはいろいろ面白い性質がある．たとえば，どのような自然数 d に対しても，フィボナッチ数列の中には 0 以外に d の倍数がある．つまり d で割り切れる $F_n\ (n>0)$ がある．

$d=11$ として表を作ってみると次のようになった．

$F_0 = 0 = 0\cdot 11 + 0$	$F_{10} = 55 = 5\cdot 11 + 0$
$F_1 = 1 = 0\cdot 11 + 1$	$F_{11} = 89 = 8\cdot 11 + 1$
$F_2 = 1 = 0\cdot 11 + 1$	$F_{12} = 144 = 13\cdot 11 + 1$
$F_3 = 2 = 0\cdot 11 + 2$	$F_{13} = 233 = 21\cdot 11 + 2$
$F_4 = 3 = 0\cdot 11 + 3$	$F_{14} = 377 = 34\cdot 11 + 3$
$F_5 = 5 = 0\cdot 11 + 5$	$F_{15} = 610 = 55\cdot 11 + 5$
$F_6 = 8 = 0\cdot 11 + 8$	$F_{16} = 987 = 89\cdot 11 + 8$
$F_7 = 13 = 1\cdot 11 + 2$	$F_{17} = 1597 = 145\cdot 11 + 2$
$F_8 = 21 = 1\cdot 11 + 10$	$F_{18} = 2584 = 234\cdot 11 + 10$
$F_9 = 34 = 3\cdot 11 + 1$	$F_{19} = 4181 = 380\cdot 11 + 1$
	$F_{20} = 6765 = 615\cdot 11 + 0$

この表から F_{10} と F_{20} は 11 で割れることがわかる．また F_0 から F_9 までを 11 で割った余りは F_{10} から F_{19} までを 11 で割った余りに等しいことに気付くであろう．よって $F_{30}, F_{40}, \cdots$ 等も 11 で割れると予想される．

F_n を 11 で割った余りを r_n としよう．すると $r_0=r_{10}, r_1=r_{11}$ で

ある．もし $r_n=r_m, r_{n+1}=r_{m+1}$ となったとき

$$\begin{aligned} r_{n+2} &= F_{n+2} && \text{を 11 で割った余り} \\ &= F_{n+1}+F_n && \text{を 11 で割った余り} \\ &= r_{n+1}+r_n && \text{を 11 で割った余り} \\ &= r_{m+1}+r_m && \text{を 11 で割った余り} \\ &= F_{m+1}+F_m && \text{を 11 で割った余り} \\ &= F_{m+2} && \text{を 11 で割った余り} \\ &= r_{m+2} \end{aligned}$$

となり $r_{n+2}=r_{m+2}$ が得られる．$r_{n+1}=r_{m+1}$ と組み合わせれば $r_{n+3}=r_{m+3}$ が得られる．以下同様にして r_n からの数列と r_m からの数列は同じになる．よって r_0 からの数列と r_{10} からの数列は同じになる．よって $0=r_{10}=r_{20}=r_{30}=r_{40}=\cdots$ が証明出来たわけである．

一般に d を定めたとき，F_n を d で割った余りを r_n とする．次に $r_n=0$ となる自然数 n が必ず見つかることを証明しよう．そのためには部屋割り論法という巧妙な方法を用いる．m 個の部屋しかないホテルに $m+1$ 人の客が泊まっているとしたら，どこかの部屋には2人(またはそれ以上)泊まっている．なぜならば，1つの部屋に1人しか泊まらないとしたら，どうしても1人はみだしてしまうからである．この単純な論法を**ディリクレの部屋割り論法**という．この論法を使うために r_n と r_{n+1} という対 (r_n, r_{n+1}) を考える．r_n は0から $d-1$ までの d 個のどれかであるから，(r_n, r_{n+1}) は $(0, 0)$, $(0, 1)$, $\cdots$, $(0, d-1)$, $(1, 0)$, $\cdots$, $(d-1, d-1)$ の d^2 個の組合せのどれかである．今，$(0, 0)$, $(0, 1)$, $\cdots$, $(d-1, d-1)$ に対応する d^2 個の部屋を作ったとする．そして，(r_n, r_{n+1}) $(0 \leqq n \leqq d^2)$ を対応する部屋に入れたとする．すると部屋は d^2 個しかなく，(r_n, r_{n+1}) の組合せは n を0から d^2 まで動かせば d^2+1 個あるので，どこかの部屋には必ずだぶることがわかる(部屋割り論法!)．そこで $(r_n, r_{n+1})=(r_m,$

$r_{m+1})$ $(n<m)$ となったとしよう．$F_{n+1}=F_n+F_{n-1}$ から

$$F_{n-1}=F_{n+1}-F_n$$

であることを利用すれば

$$\begin{aligned} r_{n-1} &= F_{n-1} && \text{を } d \text{ で割った余り} \\ &= F_{n+1}-F_n && \text{を } d \text{ で割った余り} \\ &= r_{n+1}-r_n && \text{を } d \text{ で割った余り} \\ &= r_{m+1}-r_m && \text{を } d \text{ で割った余り} \\ &= F_{m+1}-F_m && \text{を } d \text{ で割った余り} \\ &= F_{m-1} && \text{を } d \text{ で割った余り} \\ &= r_{m-1} \end{aligned}$$

となる．よって $(r_{n-1}, r_n)=(r_{m-1}, r_m)$ が得られた．同様につづければ

$$(r_0, r_1)=(r_{m-n}, r_{m-n+1})$$

となる．つまり $r_{m-n}=r_0=0$ が得られる．よって F_{m-n} が d で割れることがわかり，フィボナッチ数列の中に0以外に d の倍数があることが証明出来たわけである．

以上の証明をながめれば，d を法として考えることと部屋割り論法が上手に組み合わされていることに気付くであろう．

このほかフィボナッチ数列の中には平方数，すなわち n^2 という形になる数が $1=1^2$ と $144=12^2$ 以外にないことも証明出来るが，長い証明なので省略しよう．

§4 百五減算

江戸時代の初期に吉田光由著“塵劫記”(ジンコウキ，岩波文庫にも入っている)という優れた数学の入門書が出版された．この本の中に百五減算というものがある．これは次のような数あてゲームの1つである．

“私の年齢は3で割ると2余り，5で割ると1余り，7で割ると6余ります．さて私の年齢をあててみよ.”

このような問題を出されたとき，どのように解いたら良いだろうか．計算に慣れている人ならば，次のように強引に計算するであろう．

まず，7で割れば6余る数を1列にならべる:

$$6,\ 13,\ 20,\ 27,\ 34,\ 41,\ 48,\ 55,\ 62,\ 69,$$
$$76,\ 83,\ 90,\ 97,\ 104.$$

この数列を5で割り，余りを求める:

$$1,\ 3,\ 0,\ 2,\ 4,\ 1,\ 3,\ 0,\ 2,\ 4,$$
$$1,\ 3,\ 0,\ 2,\ 4.$$

この中で余りが1である数を拾い出す:

$$6,\ 41,\ 76.$$

この数列を3で割り，余りを求める:

$$0,\ 2,\ 1.$$

よって，求める答は41歳となる．このような強引な解き方を**目の子算**という．可能性のあるすべての場合を書き出し，条件に合わないものを徐々に消してゆき，残ったものが答である，という求め方である．確実ではあるが，時間がかかる．

“3で割った余りが a, 5で割った余りが b, 7で割った余りが c のとき，答は $-35a+21b+15c$ である”などと言われたら，目の子算で計算した人はびっくりしてしまう．$a=2, b=1, c=6$ の場合

$$-35\cdot 2+21+15\cdot 6 = -70+21+90 = 41$$

となり，この公式を使えばたちまち答が出てしまう．ただしこの公式を使うとき，答が105以上になるときは105を引き，負になったときは105を加える必要がある．$105=3\times 5\times 7$ であるから105を引いても，加えても余りには影響しないし，人間の年齢は0以上で

あり，多くの場合105以下であるからである．たとえば $a=0, b=4, c=6$ のときは

$$-35a+21b+15c = 21\cdot4+15\cdot6 = 174,$$
$$174-105 = 69$$

となり，69歳が答となる．このように105を越えたとき，105を引くので**百五減算**と呼ばれるわけである．

では何故この公式は正しいのだろうか．$-35=-36+1$ であることを考えると

$$\begin{aligned}-35a+21b+15c &= -36a+21b+15c+a \\ &= 3\cdot(-12a+7b+5c)+a\end{aligned}$$

となり，3で割れば a 余ることがわかる．同様に

$$\begin{aligned}-35a+21b+15c &= 5\cdot(-7a+4b+3c)+b \\ &= 7\cdot(-5a+3b+2c)+c\end{aligned}$$

となり，5で割れば b 余り，7で割れば c 余ることがわかる．よってこの公式は正しい．

さて，この公式を知らないとき，目の子算ではない一般的な解き方を次に紹介しよう．

答を n 歳とすれば

(1) $$n = 3x+2$$

(2) $$n = 5y+1$$

(3) $$n = 7z+6$$

となる整数 x, y, z があるはずである．(1), (2) から $3x+2 = 5y+1$，つまり

(4) $$3x-5y = -1$$

となる．

(5) $$3\cdot2-5\cdot1 = 1$$

であるから，(4) と (5) を加えて

(6) $$3(x+2) = 5(y+1)$$

となる．(6)の左辺が5で割れるということは，$x+2$ が5で割れなければならない．よって

(7) $$x+2 = 5t$$

となる整数 t がなければいけない．(7)を(1)に代入すると

(8) $$n = 3(5t-2)+2 = 15t-4$$

となる．(3)と(8)から $7z+6=15t-4$，つまり

(9) $$7z-15t = -10$$

となる．

(10) $$7\cdot 2-15\cdot 1 = -1$$

であるから両辺を10倍して

(11) $$7\cdot 20-15\cdot 10 = -10$$

となり(9)と(11)から

(12) $$7(z-20) = 15(t-10)$$

となる．左辺が15で割れるためには $z-20$ が15で割れなければいけない．よって

(13) $$z-20 = 15s$$

となる整数 s がある．(13)を(3)に代入すれば

(14) $$n = 7(15s+20)+6$$
$$= 146+105s$$

となる．年齢は普通105より小さいから $s=-1$ とおけば $a=41$ となる．

以上の解法を吟味すると，(5), (10)のように右辺が ± 1 になる組合せを見つけることが大切である．次に(6)から(7)，(12)から(13)を導く所が大切である．一般に b と c に共通の約数が1以外にないとき**互いに素**という．このとき，もし ab が c で割れれば a が c で割れる．この事実は後に正確に証明しよう．また(5), (10)のような

組合せを見つける一般的な計算法も，次章に示そう．

§5　循環小数

まず1を7で割ってみよう．6回計算すると余りとして1が現われる．よってこの計算をつづければ，同じ数字が繰り返し現われるはずであるから，計算をこれ以上つづけなくとも答はわかる．このとき，小数の表わし方として

$$
\begin{aligned}
1/7 &= 0.142857\,142857\cdots \\
&= 0.\dot{1}4285\dot{7}
\end{aligned}
$$

```
     0.142857
  7)1.000000
      7
     30
     28
      20
      14
       60
       56
        40
        35
         50
         49
          1
```

のように繰り返し現われる数字のはじめと終りの上に黒い点・をつけることにする．この・から・までを**循環節**といい，このような数を**循環小数**という．ところで142857には不思議な性質がある．まずそれに2, 3, …, 6をそれぞれ掛けると答は142857の順が替るだけである．

$$
\begin{aligned}
142857\times 2 &= 285714 \\
142857\times 3 &= 428571 \\
142857\times 4 &= 571428
\end{aligned}
$$

$$142857 \times 5 = 714285$$

$$142857 \times 6 = 857142.$$

また前半と後半を加えると 142+857=999 となる．このような性質は他の数にもある．たとえば 1 を 17 で割ると

$$1/17 = 0.\dot{0}58823529411764\dot{7}$$

となり，0.0588235294117647 に $2, 3, \cdots, 16$ のそれぞれを掛けると同じように順が替る：

$$0588235294117647 \times 2 = 1176470588235294$$

$$0588235294117647 \times 3 = 1764705882352941$$

$$0588235294117647 \times 4 = 2352941176470588$$

$$0588235294117647 \times 5 = 2941176470588235$$

$$0588235294117647 \times 6 = 3529411764705882$$

$$0588235294117647 \times 7 = 4117647058823529$$

$$0588235294117647 \times 8 = 4705882352941176$$

$$0588235294117647 \times 9 = 5294117647058823$$

$$0588235294117647 \times 10 = 5882352941176470$$

$$0588235294117647 \times 11 = 6470588235294117$$

$$0588235294117647 \times 12 = 7058823529411764$$

$$0588235294117647 \times 13 = 7647058823529411$$

$$0588235294117647 \times 14 = 8235294117647058$$

$$0588235294117647 \times 15 = 8823529411764705$$

$$0588235294117647 \times 16 = 9411764705882352.$$

また前半と後半を加えると 9 が並ぶ：

$$05882352 + 94117647 = 99999999.$$

1000 以下の数で上と同じ性質を持つ数が 60 個ある．それらは

7，17，19，23，29，47，59，61，97，109，113，

131，149，167，179，181，193，223，229，233，

257, 263, 269, 313, 337, 367, 379, 383, 389,
419, 433, 461, 487, 491, 499, 503, 509, 541,
571, 577, 593, 619, 647, 659, 701, 709, 727,
743, 811, 821, 823, 857, 863, 887, 937, 941,
953, 971, 977, 983

である．たとえば1を983で割ると982回割り算をするとやっと循環しはじめる．循環節を2, 3, …, 982倍すると順が替わるだけであり，また前半と後半を加えると9が491個並ぶ．何故であろうか．

```
    0.714285            0.142857
  7)5.000000          7)1.000000
    4 9                 7
     10                 *30
      7                  28
     30                  *20
     28                   14
      20                  *60
      14                   56
       60                  *40
       56                   35
        40                  *50
        35                   49
         5                   *1
```

1を7で割った場合を考えると割り算の余りが3, 2, 6, 4, 5, 1となり1から6までのすべての数が現われる．よってたとえば5を7で割ると，その計算は1を7で割ったときの途中から始まるだけで，以後は同じ計算がつづく．つまり商は142857の順が替っただけである．

ところで，1を7で割った計算の意味を考えれば

$$10^6 = 7\times 142857+1$$

であることがわかる．両辺を5倍すれば

$$5\cdot 10^6 = 7\times(5\times 142857)+5$$

となる．他方，5を7で割る計算を見れば

$$5\cdot10^6 = 7\times714285+5$$

となり，この2式から

$$5\times142857 = 714285$$

が得られる．右辺は142857の順が替っただけであることは，計算を実行する前から保証されている．このようにして142857を5倍しても順が替わるだけであることが説明出来た．大切なことは，1を7で割っていくとき，余りとして1から6までの数がすべて現われることである．

次に前半と後半を加えるとなぜ999と9が並ぶのであろうか．1を7で割るとき，6回目にやっと1が現われる．つまり，iが6より小さければ10^i-1は7で割り切れない．10^6-1は7で割れるから$(10^3-1)(10^3+1)$も7で割れる．10^3-1は7で割れないから10^3+1が7で割れる．つまり10^3-6が7で割れる．事実3回目に余りとして6が現われ，割り算の計算の仕方から

$$10^3 = 6+7\times142$$

$$6\cdot10^3 = 1+7\times857$$

となる．両式を加えると

$$7\cdot10^3 = 7+7\times(142+857)$$

となる．両辺を7で割ると

$$142+857 = 10^3-1 = 999$$

となる．よって前半と後半を加えると9が並ぶことの説明が出来た．

以上の説明をながめると，iが6より小さければ10^i-1が7で割れないことが本質的な原因であることがわかる．このようなとき，10は7の**原始根**であるという．

§6 角谷予想

或る2以上の自然数から出発して次の2つの操作を行なったとする:

(1) 奇数ならば3倍して1を加える.

(2) 偶数ならば2で割る.

たとえば，3から出発すれば

(3) $$3 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1$$

となり最後には1になる. 7から出発すると

(4) $$7 \to 22 \to 11 \to 34 \to 17 \to 52 \to 26 \to 13 \to 40 \to 20 \to 10$$

となり10以後は(3)の2番目から進み，最後に1になる. しかし27から出発すると大変な計算になる:

(5) $$\begin{aligned}&27\to82\to41\to124\to62\to31\to94\to47\to142\to71\to214\\&\to107\to322\to161\to484\to242\to121\to364\to182\to91\\&\to274\to137\to412\to206\to103\to310\to155\to466\to233\\&\to700\to350\to175\to526\to263\to790\to395\to1186\to593\\&\to1780\to890\to445\to1336\to668\to334\to167\to502\\&\to251\to754\to377\to1132\to566\to283\to850\to425\\&\to1276\to638\to319\to958\to479\to1438\to719\to2158\\&\to1079\to3238\to1619\to4858\to2429\to7288\to3644\\&\to1822\to911\to2734\to1367\to4102\to2051\to6154\\&\to3077\to9232\to4616\to2308\to1154\to577\to1732\to866\\&\to433\to1300\to650\to325\to976\to488\to244\to122\\&\to61\to184\to92\to46\to23\to70\to35\to106\to53\to160\\&\to80\to40\end{aligned}$$

となり，やっとのことで(4)の後から3番目となった. よって最後には1となる.

さて，どのような奇数から出発しても(1), (2)の操作を繰り返せ

ば必ず1になる，という予想がある．誰が言いだしたかわからないが，この予想がアメリカの或る数学研究所に伝わると易しそうな問題だからすぐ解けるであろうと皆が考え，証明しようと試みる．しかしなかなか解けないのでその研究所の機能が1週間ほど停止する．1週間もすると，誰しも証明をあきらめ，この問題は他の研究所に伝わる．するとその研究所も1週間ほど機能を停止する．…このような伝説のある予想である．十数年ほど前に日本へは角谷静夫教授により伝えられたので，日本では**角谷予想**と呼ばれている．まだ誰もこの予想の証明に成功していない．7000億以下の数に対してはこの予想が正しいと確かめられている(米田信夫教授による計算)．

初等整数論には，問題の意味は少し説明すれば誰にもわかるけれど，しかし誰も証明することの出来ない問題が多い．昔から知られている世界であり，しかも底知れぬ深さを持った世界である．

第2章　ユークリッドの互除法

§1　約数と倍数

まずはじめに言葉の復習をしよう．**自然数**とは $1, 2, 3, \cdots$ という一番素朴な数である．物の個数や順序を表わすものとして自然に生まれてきた言葉である．自然数 a と b を加えても自然数だけれど，一般に引き算 $a-b$ は $a>b$ でなければ自然数の範囲で出来ない．これでは不便であるから，**ゼロ** 0 および**負の整数** $-1, -2, -3, \cdots$ を人間は考え出した．自然数，ゼロおよび負の整数をまとめて**整数**という．これから扱う数は主に自然数または整数であるから，特にことわらないかぎり数とは自然数または整数を意味するものとする．まとめると

$$\text{整数}\begin{cases}\text{負でない整数}\begin{cases}\text{正の整数} = \text{自然数} = 1, 2, 3, \cdots \\ \text{ゼロ} = 0\end{cases} \\ \text{負の整数} = -1, -2, -3, \cdots\end{cases}$$

となる．

人間が何か計算しているとき，具体的には必ず整数の四則計算を行なっている．整数の加減乗除を組み合せてすべての計算は行なわれる．だから整数の四則算法の性質を良く調べることは大切だし，またいろいろ面白い現象が現われてくる．いろいろな性質を正確に表現するために，いろいろな数学的な言葉をはっきりさせよう．

整数 a に対してその**絶対値** $|a|$ を次のように定義する．

$$|a| = a\text{の絶対値} = \begin{cases} a, & a \geqq 0 \text{ のとき} \\ -a, & a < 0 \text{ のとき}\end{cases}$$

たとえば $|3|=3$, $|-5|=5$ である．この定義からすべての整数 a に対

して $|a| \geqq 0$ であり，$|a|=0$ となるのは $a=0$ のときだけである．

さて，整数の範囲で足し算，引き算，掛け算は自由に出来るが，しかし割り算はいつもは出来ない．つまり $a, b (b \neq 0)$ を整数としたとき，$a \div b$ は整数とは限らない．しかし

(1) $$a = b \cdot q + r, \quad 0 \leqq r < |b|$$

となる q および r はただ1通り存在する．たとえば

$$15 = 4 \times 3 + 3 \qquad (q=3,\ \ r=3)$$

$$-15 = 4 \times (-4) + 1 \qquad (q=-4,\ \ r=1)$$

となる．q を**商**といい，r を**余り**という．この性質は整数の一番基本的なものである．他のいろいろな性質はこの基本的な性質を土台にして説明される．よってこの基本的な性質を正確に証明しよう．

まず，(1)のように表わされることを示そう．$a>0, b>0$ の場合を考えよう．

a に関する帰納法を用いることにしよう．a に関する帰納法とは

（イ） $a=1$ のときは成り立つ，

（ロ） $a=n$ のとき成り立てば，$a=n+1$ のときも成り立つ，

という2つのことを使って証明する方法である．(イ)から $a=1$ のときは成り立つから，(ロ)において $n=1$ とおけば $a=2$ のときも成り立つ．ふたたび(ロ)において $n=2$ とおけば $a=3$ のときも成り立つ．この操作を限りなくつづければ，a の値がどのような自然数でも成り立つ．このような証明法を**帰納法**という．神のような無限のかなたまで見通せる心境でこの証明法を吟味すると，(ロ)という操作を無限回用いれば，a がどのような自然数に対しても証明が終っていることに気付くであろう．

さて実際にこの証明法を用いて(1)を試してみよう．$a=1$ のときは，

$$1 = b \cdot 1 + 0 \qquad (1=b \text{ の場合})$$

$$= b\cdot 0+1 \qquad (1<b\text{ の場合})$$

でよい．$a=n$ まで成り立ち

$$n = b\cdot q+r, \qquad 0 \leqq r < b$$

のとき，$0<r+1\leqq b$ であるから

$$n+1 = \begin{cases} b\cdot q+(r+1) & (r+1<b\text{ の場合}) \\ b(q+1)+0 & (r+1=b\text{ の場合}) \end{cases}$$

となり，$a>0, b>0$ の場合は(1)と表わされることが示された．$a>0, b<0$ の場合は $|b|>0$ であるから

$$a = |b|\cdot q+r, \qquad 0 \leqq r < |b|$$

となる q, r は見つかるので

$$a = b\cdot(-q)+r, \qquad 0 \leqq r < |b|$$

となり，(1)が成り立つ．次に $a=0$ の場合は

$$0 = b\cdot 0+0$$

でよい．$a<0$ の場合は $|a|>0$ であるから

$$|a| = b\cdot q+r, \qquad 0 \leqq r < |b|$$

と表わされる．よって

$$\begin{aligned} a &= b(-q)-r \\ &= \begin{cases} b(-q)+0 & (r=0\text{ の場合}) \\ b(-q-1)+(b-r) & (0<r<b\text{ の場合}) \\ b(-q+1)+(-b-r) & (0<r<-b\text{ の場合}) \end{cases} \end{aligned}$$

となり，どの場合も(1)と表わされることがわかった．

次にこの割り算がただ1通りであることを示そう．もし

$$\begin{aligned} a &= b\cdot q+r, & 0 &\leqq r < |b| \\ &= b\cdot q'+r', & 0 &\leqq r' < |b| \end{aligned}$$

とすると

$$(2) \qquad b(q-q') = r'-r, \qquad -|b| < r'-r < |b|$$

となる．もし $q\neq q'$ とすると(2)の左辺の絶対値は

$$|b|\cdot|q-q'| \geqq |b| > |r'-r|$$

となり矛盾である．よって $q=q'$ となり，(2)から $r=r'$ となる．つまりただ1通りにしか表わせないことがわかった．

ところで $r=0$ のとき，つまり a が b で割り切れて $a=b\cdot q$ となるとき，b を a の**約数**といい，a を b の**倍数**という．$a=b\cdot q$ のとき $a=(-b)\cdot(-q)$ であるから，b が a の約数ならば $-b$ も a の約数である．よって a が自然数のとき，a の約数として自然数のみを普通考える．

例　28のすべての約数を求めよ．また28の約数で28より小さい数の和を求めよ．

解
$$\begin{aligned}28 &= 1\times 28\\ &= 2\times 14\\ &= 3\times 8+4\\ &= 4\times 7\\ &= 5\times 5+3\end{aligned}$$

となるので，6以上で割っても商は4以下になる．よってこれ以上計算する必要はなく，約数は

$$1,\ 2,\ 4,\ 7,\ 14,\ 28$$

となる．1および28も約数である．28以外の約数の和は

$$1+2+4+7+14 = 28$$

となり元の数28と同じになる．——

§2　公約数，最大公約数

2つの整数 a, b のうちどちらかは0でないとしておく．a の約数でもあり，同時に b の約数でもある数を a と b の**公約数**という．たとえば $a=1\cdot a$, $b=1\cdot b$ であるから，1は a と b の公約数である．$b\neq 0$ のとき b の約数 c に対して $b=c\cdot q$ となる $q\ (\neq 0)$ がある．よっ

て $c \leqq |c|\cdot|q|=|b|$ となる．よって a と b の公約数 c に対しても $c \leqq |b|$ である．このように公約数の大きさは制限されているから，公約数の中で最大な公約数が定まる．この最大な公約数のことを**最大公約数**といい，記号で (a, b) と書く．

例 $a=42, b=28$ の最大公約数を求めよ．

解

$$\begin{aligned} 42 &= 1\times 42 \\ &= 2\times 21 \\ &= 3\times 14 \\ &= 4\times 10+2 \\ &= 5\times 8+2 \\ &= 6\times 7 \end{aligned}$$

から 42 の約数は

$$1,\ 2,\ 3,\ 6,\ 7,\ 14,\ 21,\ 42$$

となる．また，28 の約数は

$$1,\ 2,\ 4,\ 7,\ 14,\ 28$$

であるから 42 と 28 の公約数は

$$1,\ 2,\ 7,\ 14$$

となる．この中で最大な数は 14 である．よって

$$(42, 28) = 14$$

となる．——

例 $a=0, b \neq 0$ のとき最大公約数を求めよ．

解 b の約数の中で最大な数は $|b|$ である．$0=|b|\cdot 0$ であるから $|b|$ は 0 の約数でもある．よって

$$(0, b) = |b| \qquad (b \neq 0)$$

となる．——

§3 ユークリッドの互除法

2つの自然数 a, b が与えられたとき，その最大公約数 (a, b) を求めるにはどうしたら良いだろうか．割り算を何度も実行し，a の約数をすべて求め，b の約数もすべて求めれば良いけれど，これは a, b が大きいと大変な計算となる．後に述べるように，a と b を素因子分解すれば良いけれど，素因子分解するのも楽ではない．たとえば $a=4676, b=1141$ のとき

$$a = 2\cdot 2\cdot 7\cdot 167, \qquad b = 7\cdot 163$$

と素因子分解すれば $(a, b)=7$ とわかるが，$a=8633, b=5429$ のときなど素因子分解するのは大変である．ところがギリシャ時代にユークリッド(330?–275? B.C.)の書いた“幾何学原論”の中に，非常に優れた方法が書かれている．その方法とは

“$a = b\cdot q+r$，とすると，

$(a, b) = (b, r)$ となる”

という事実を何回も使うことである．たとえば上の $a=4676, b=1141$ の場合，

$$4676 = 1141\times 4+112$$

であるから，$(4676, 1141)=(1141, 112)$ が得られる．

同様に

$$1141 = 112\times 10+21$$
$$112 = 21\times 5+7$$
$$21 = 7\times 3+0$$

であるから

$$(1141, 112) = (112, 21) = (21, 7) = (7, 0) = 7$$

となり，4676 と 1141 の最大公約数は 7 が得られた．同様に 8633 と 5429 の最大公約数は

$$8633 = 5429\times 1+3204$$

$$\begin{aligned}5429 &= 3204\times1+2225\\3204 &= 2225\times1+\ 979\\2225 &= \ 979\times2+\ 267\\979 &= \ 267\times3+\ 178\\267 &= \ 178\times1+\ \ 89\\178 &= \ \ 89\times2+\ \ \ 0\end{aligned}$$

から$(8633, 5429)=89$が得られた．よって89は8633および5429の約数である．よって

$$8633 = 89\times97, \qquad 5429 = 89\times61$$

と素因子分解することが出来る．素因子分解は大変だが，最大公約数を見つけるのは自動的で容易なので，aの素因子を求めるのに，何とかして$(a, b)>1$となる適当なbを見つける工夫が，良く使われる．

さて“原論”に書かれているこの方法を正当化しよう．aとbの最大公約数をdとし，$a=d\cdot a', b=d\cdot b'$としよう．このとき

$$\begin{aligned}r &= a-b\cdot q\\&= d\cdot a'-d\cdot b'\cdot q\\&= d\cdot(a'-b'\cdot q)\end{aligned}$$

となりdはrの約数でもある．dはbの約数でもあるから，dはbとrの公約数である．bとrの最大公約数をd_1とすればd_1は公約数の中で最大であるから，$d\leqq d_1$となる．

逆に$d_1=(b, r)$はbとrの公約数であるから，$b=d_1\cdot b'', r=d_1\cdot r''$となり

$$\begin{aligned}a &= b\cdot q+r\\&= d_1\cdot b''\cdot q+d_1\cdot r''\\&= d_1\cdot(b''\cdot q+r'')\end{aligned}$$

となりd_1はaの約数となる．よってd_1はaとbの公約数となり，

$d_1 \leqq d$ となる．

以上で $d=d_1$ となる．まとめると次の定理のような形になる．

定理 1　自然数 a, b に対し

$$a=b\cdot q+r \quad ならば \quad (a, b)=(b, r)$$

となる．——

この定理 1 を使って最大公約数を求める方法を，**ユークリッドの互除法**という．（略して**互除法**ともいう．）

ユークリッドの互除法の計算を逆にたどると面白いことがわかる．たとえば $7=(4676, 1141)$ の計算から

$$\begin{aligned} 7 &= 112-21\times5 \\ &= 112-(1141-112\times10)\times5 \\ &= 112\times51-1141\times5 \\ &= (4676-1141\times4)\times51-1141\times5 \\ &= \mathbf{4676}\times51-\mathbf{1141}\times209 \end{aligned}$$

となる．また $89=(8633, 5429)$ の計算からは

$$\begin{aligned} 89 &= 267-178 \\ &= 267-(979-267\times3) \\ &= 267\times4-979 \\ &= (2225-979\times2)\times4-979 \\ &= 2225\times4-979\times9 \\ &= 2225\times4-(3204-2225)\times9 \\ &= 2225\times13-3204\times9 \\ &= (5429-3204)\times13-3204\times9 \\ &= 5429\times13-3204\times22 \\ &= 5429\times13-(8633-5429)\times22 \\ &= \mathbf{5429}\times35-\mathbf{8633}\times22 \end{aligned}$$

が得られる．いつでもこのように逆に計算がたどれるので次の定理

が得られた．

定理 2　自然数 a, b の最大公約数を d とすると

$$d = a\cdot x + b\cdot y$$

となる整数 x, y が存在する．——

ユークリッドの互除法を用いれば，定理2の x, y を具体的に計算することが出来る．このように互除法は強力な計算法なのである．

例　$1=17x+13y$ となる x, y を求めよ．

解　互除法を実行すると

$$17 = 13\times 1+4$$
$$13 = \ 4\times 3+1$$

であるから $(17, 13)=1$ である．よって解は存在する．

この計算から

$$\begin{aligned} 1 &= 13-4\times 3 \\ &= 13-(17-13)\times 3 \\ &= 13\times 4-17\times 3. \end{aligned}$$

よって $x=-3, y=4$ となる．——

例　a と b の公約数 c は $(a, b)=d$ の約数である．

解　定理2から

$$d = ax+by$$

となる整数 x, y がある．c は公約数であるから $a=c\cdot a', b=c\cdot b'$ となる．よって

$$\begin{aligned} d &= c\cdot a'\cdot x+c\cdot b'\cdot y \\ &= c(a'\cdot x+b'\cdot y) \end{aligned}$$

から c は d の約数となる．——

$(b, c)=1$ のとき b と c とは**互いに素**である，という．つまり自明な1以外に公約数がないわけである．b は c と**素**，または c は b と**素**，などということもある．このとき定理2から

(1) $$1 = bx+cy$$

となる整数 x と y が存在する．このとき ab が c で割れれば a が b で割れることを示そう．(1)の両辺に a を掛けると

$$a = abx+acy$$

となる．もし c が ab の約数ならば $ab=c\cdot c'$ と書ける．よって

$$\begin{aligned} a &= c\cdot c'x+acy \\ &= c(c'x+ay) \end{aligned}$$

となり c は a の約数である．つまり次の定理が得られた．

定理 3　c が ab の約数であり $(b, c)=1$ ならば c は a の約数である．

例　13 で割ると 7 余り，17 で割ると 14 余る数を求めよ．

解　求める答を n とすれば

(2) $$n = 13x+7$$

(3) $$n = 17y+14$$

となる整数 x, y がある．よって

$$13x+7 = 17y+14$$

(4) $$13x-17y = 7$$

となる．前の例から

(5) $$13\times 4-17\times 3 = 1$$

であったから，(5)の両辺を 7 倍し(4)から引くと

$$13(x-28) = 17(y-21)$$

となる．左辺は 17 で割れ，13 と 17 は互いに素であるから $(x-28)$ が 17 で割れる．つまり

$$x-28 = 17z$$

となる整数 z がある．(2)に代入すると

$$\begin{aligned} n &= 13(17z+28)+7 \\ &= 221z+371 \end{aligned}$$

$$= 221(z+1)+150.$$

よって150が最小な自然数解であり，これに$221=13\times 17$の倍数を加えても答である．——

§4　不定方程式

前節の例のように，たとえば

$$17x+13y = 1$$

の整数解をすべて求めるにはどうしたら良いだろうか．一般に整数a, b, cが与えられたとき

(1)
$$ax+by = c$$

となる整数解x, yはあるだろうか．あるとしたら解をすべて求めるにはどうしたら良いだろうか．

まず$d=(a, b)$とおく．よって$a=da_1, b=db_1$となる．(1)にもし解があったならば

$$\begin{aligned} c &= da_1x+db_1y \\ &= d(a_1x+b_1y) \end{aligned}$$

となり，cはdで割れなければならない．つまり(1)に解があるためにはcがdの倍数となることが必要である．

逆にcがdの倍数とする．定理2から

(2)
$$d = ax_1+by_1$$

となる整数解x_1, y_1が存在する．$c=dc_1$のとき，(2)の両辺をc_1倍すると

$$\begin{aligned} c &= dc_1 \\ &= a(x_1c_1)+b(y_1c_1) \end{aligned}$$

となる．よって$x=x_1c_1$，$y=y_1c_1$とおけば，(1)の解となる．つまりcがdの倍数となることは，(1)が解を持つために十分な条件である．

さて c が d の倍数のとき，ユークリッドの互除法で(2)の x_1, y_1 を計算出来るので，(1)の１組の解が計算出来る．ではすべての解を求めるにはどうしたら良いだろうか．x', y' を他の解とすれば

$$ax'+by' = c \tag{3}$$

となる．(1)から(3)を引くと

$$a(x-x') = b(y'-y) \tag{4}$$

が得られる．$d=(a, b), a=da_1, b=db_1$ とおくと $(a_1, b_1)=1$ となる．なぜならもし a_1 と b_1 に１より大きな公約数 d_1 があり $a_1=d_1\cdot a_2, b_1=d_1\cdot b_2$ となったとすると $a=(dd_1)a_2, b=(dd_1)b_2$ となり dd_1 が a と b の公約数となる．これは d が最大な公約数であることに反する．よって $(a_1, b_1)=1$ である．

(4)の両辺を d で割ると

$$a_1(x-x') = b_1(y'-y), \qquad (a_1, b_1) = 1 \tag{5}$$

となる．(5)の右辺は b_1 の倍数であるから，左辺も b_1 で割れる．しかし $(a_1, b_1)=1$ であるから定理３から $x-x'$ が b_1 で割れなければならない．よって

$$x-x' = b_1\cdot t$$

とならなければいけない．このとき，

$$a_1\cdot b_1\cdot t = b_1(y'-y)$$

であるから両辺を b_1 で割り

$$a_1\cdot t = y'-y$$

でなければならない．つまり他に解があったとすると，

$$x' = x-b_1t, \qquad y' = y+a_1t \tag{6}$$

という形をしていなければならない．

逆に x', y' が(6)の形をしていれば，

$$\begin{aligned} ax'+by' &= a(x-b_1t)+b(y+a_1t) \\ &= (ax+by)+(-a\cdot b_1+b\cdot a_1)t \end{aligned}$$

$$= c+(-da_1\cdot b_1+db_1\cdot a_1)t$$
$$= c$$

となり(1)の解となる．つまり(6)が解のすべてである．

例　$17x+13y=5$ のすべての解を求めよ．

解　$(17,13)=1$ であり，5は自明な約数1を持つから解はある．前節の例から

$$17(-3)+13\cdot 4 = 1$$

となる解が見つかるので，両辺を5倍して

$$17\cdot(-15)+13\cdot 20 = 5$$

となる．よってすべての解(一般解)は(6)から

$$x = -15-13t$$
$$y = 20+17t$$

となる．——

このように解が1組に定まらず，無限に多くあるので(1)のような方程式を1次の**不定方程式**という．

例　$21x+15y=2$ を解け．

解　$(21,15)=3$ であり，2は3の倍数でないので解は存在しない．——

例　$21x+15y=9$ を解け．

解　$(21,15)=3$ であり，9は3の倍数なので解はある．問題の両辺を3で割れば

$$7x+5y = 3$$

となる．互除法を用いると

$$7 = 5\cdot 1+2$$
$$5 = 2\cdot 2+1$$

であるから

$$1 = 5-2\cdot 2$$

$$= 5-(7-5\cdot 1)\cdot 2$$
$$= 5\cdot 3-7\cdot 2$$

となる．両辺を3倍して

$$3 = 5\cdot 9+7\cdot(-6)$$

となる．よって一般解は

$$x = -6-5t$$
$$y = 9+7t$$

となる．——

§5　何回割り算が必要か

a, b を $a \geqq b$ でかつ10000以下の自然数とする．そのとき互除法で a と b との最大公約数を求めるには，何回割り算を実行したら良いだろうか．a が b の倍数の場合はただ1回割り算を行なえば良い．しかし最も手間がかかる場合は何回だろうか．つまり

$$\begin{aligned} a &= b\cdot q_1+r_1, & 0 &< r_1 < b \\ b &= r_1\cdot q_2+r_2, & 0 &< r_2 < r_1 \\ r_1 &= r_2\cdot q_3+r_3, & 0 &< r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1}\cdot q_n+r_n, & 0 &= r_n \end{aligned}$$

としたときの n の最大値を求めたい．そのために逆に n を固定したときの a の最小値を求めてみよう．$b \leqq a$, $r_{i+1}<r_i$ であるから $q_1, q_2, \cdots, q_n$ は1以上である．特に $r_n=0$ から q_n は2以上である．よって a が最小になる場合は $r_{n-1}=1, q_n=2, q_{n-1}=q_{n-2}=\cdots=q_1=1$ の場合である．このとき

$$r_{n-1} = 1,\ r_{n-2} = 2,\ r_{n-3} = r_{n-2}+r_{n-1},\ \cdots,\ a = b+r_1$$

となり $F_2=1, F_3=2, F_{n+2}=F_{n+1}+F_n$ となるフィボナッチ数列

$$1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144,$$

233, 377, 610, 987, 1597, 2584, 4181,

6765, 10946, …

が得られる．この数列から $n \geqq 19$ ならば $a \geqq 10946$ であることがわかる．つまり割り算が 19 回必要となるのは $a \geqq 10946$ の場合だけである．よって $a < 10000$ ならば 18 回以下しか割り算は必要でない．しかし 18 回必要なこともある．たとえば $a=6765, b=4181$ のときには，割り算は確かに 18 回必要である．10946 は $F_{21} = F_{18+3}$ である．

以上の考察から $b \leqq a < F_{n+3}$ のとき最大公約数を求めるには，最も手間がかかる場合でも n 回割り算を実行すれば良いことがわかった．証明は省略するが，F_n の大きくなる割合を正確に評価すると

$$n \leqq 5 \times (a\text{ の桁数}) - 1 \qquad \text{（ラメの定理）}$$

あるいはもう少し精密に

$$n \leqq 4.79 \times (a\text{ の桁数}) - 0.37$$

であることがわかる．たとえば $1000 \leqq a < 10000$ とすれば，a は 4 桁であるから

$$n \leqq 4.79 \times 4 - 0.37 = 18.79$$

となり，18 回以下の割り算を実行すれば，互除法で最大公約数が求まる．また a, b が 100 桁ほどの大きな数であっても，500 回以下の割り算で最大公約数が求まる．よって電子計算機で大きな数の最大公約数を求めるとき，どのくらいの時間で計算が終るか評価出来る．そしてその時間は問題にならないくらい短い時間であることがわかる．

§6 公倍数，最小公倍数

2 つの自然数 a, b に対して，a の倍数でもあり，同時に b の倍数でもある数を a と b の**公倍数**という．たとえば $a \cdot b$ は a と b の公倍

数である．$a=10, b=15$ のとき $a\cdot b=150$ は確かに 10 と 15 の公倍数であるが，30 も 10 と 15 の公倍数である．0 はいつでも a と b の公倍数である．普通，倍数というと正な倍数を意味する．公倍数の中で最小の数を**最小公倍数**という．

例　$a=10, b=15$ のとき a の倍数は

$$10,\ 20,\ 30,\ 40,\ 50,\ 60,\ 70,\ 80,\ 90,\ 100,\ \cdots$$

b の倍数は

$$15,\ 30,\ 45,\ 60,\ 75,\ 90,\ 105,\ 120,\ 135,\ 150,\ \cdots$$

となる．よって公倍数は

$$30,\ 60,\ 90,\ 120,\ 150,\ \cdots$$

となり，最小公倍数は 30 である．——

a と b が与えられたとき，最小公倍数を計算するにはどうしたら良いだろうか．次に最大公約数が求まれば，最小公倍数は容易に求まることを示そう．最大公約数 $d=(a, b)$ は互除法で求まる．このとき $a=d\cdot a'$, $b=d\cdot b'$ となり $(a', b')=1$ である．m を a と b のある公倍数とする．m は a で割れるから $m=a\cdot m'=d\cdot a'\cdot m'$ となる．m は $b=d\cdot b'$ でも割れるから，$a'\cdot m'$ は b' で割れる．$(a', b')=1$ であるから定理 3 から m' は b' で割れて $m'=b'\cdot m''$ と書ける．よって $m=d\cdot a'\cdot b'\cdot m''$ という形をしていなければいけない．ところが $d\cdot a'\cdot b'\cdot m''=a\cdot(b'\cdot m'')=b\cdot(a'\cdot m'')$ となるから，このような形をしていれば必ず公倍数である．また $m''=1$ のときが最小である．つまり $d\cdot a'\cdot b'=a\cdot b/d$ が最小公倍数である．したがって次のようにまとめられる．

定理 4　a と b の最大公約数を d, 最小公倍数を m とすると $m=a\cdot b/d$ となる．すべての a と b の公倍数は m の倍数である．——

第3章 素　　数

§1　素数と合成数

a を2以上の自然数とする．$a=1\times a$ であるから a には1と a の2つの約数がある．もしこの2つだけしか約数がないとき，a を**素数**という．3つ以上の約数があるときは a を**合成数**という．1には約数が1だけしかないから素数でも合成数でもない．a を合成数とすると $1, a$ 以外の約数 b がある．このとき $a=b\cdot c$ $(1<b)$ とすると $b\neq a$ から $c\neq 1$ である．よって $b<bc=a$ となる．つまり1より大きく，a より小さい約数がある．

例　2より小さく，1より大きい自然数はない．よって2は素数である．2は最小の素数である．2以外の素数は奇数であるから**奇素数**という．——

例　3より小さく，1より大きい自然数は2である．3は2で割り切れないから3は素数である．——

例　$4=2\times 2$ である．よって4は合成数である．4は最小の合成数である．——

例　5より小さく，1より大きな自然数は $2, 3, 4$ である．5はこれらで割り切れないから素数である．——

一般に3以上の自然数 a が与えられたとき，素数か合成数か判定するにはどうしたら良いだろうか．a がもし合成数ならば，$a=b\cdot c$, $1<b<a, 1<c<a$ となる．b と c を比べ，かりに $b\leqq c$ としよう．よって $1<b\leqq c<a$ となる．$b\leqq c$ から $b^2\leqq b\cdot c=a$，つまり $b\leqq\sqrt{a}$ である．よって2以上，$\sqrt{a}$ 以下の数で割り切れなければ，a は素数となる．よって a を $2, 3, 4, \cdots$ と a より小さな数で割っていく：

$$a = 2\cdot q_2+r_2, \quad 0 < r_2 < 2$$
$$a = 3\cdot q_3+r_3, \quad 0 < r_3 < 3$$
$$a = 4\cdot q_4+r_4, \quad 0 < r_4 < 4$$
$$\vdots$$

このようにしていくとき，もし余りが0となるときがあればaは合成数である．順に計算していき，aをmで割ったときの余りr_mが0でなく，商q_mが$q_m \leqq m$となったとき，$r_m < m$であるから

$$(m+1)^2 = m^2+2m+1 > m\cdot q_m+2r_m+1$$
$$> m\cdot q_m+r_m = a$$

つまり$m+1>\sqrt{a}$となる．aが合成数ならば，$\sqrt{a}$以下の数で割り切れるはずだから，これ以上割り算を実行しなくともよい．つまりaは素数と判定出来る．

例
$$7 = 2\cdot 3+1 \qquad (q_2=3,\ r_2=1)$$
$$= 3\cdot 2+1 \qquad (q_3=2<3,\ r_3=1).$$

3で割ったときの商が3以下だから，7は素数である．——

例　$8=2\times 2\times 2$, $9=3\times 3$, $10=2\times 5$であるから8, 9, 10は合成数である．まとめると10以下の素数は2, 3, 5, 7の4つである．——

aを合成数とし，1以外の最小の約数をbとする．このときbは素数である．なぜならば$b=c\cdot d$, $1<c<b$となったとすると，cはaの約数であり，bより小さいので，bが最小であることに反する．よって$\sqrt{a}$以下の素数で割れなければ，aは素数である．$a<100$のとき，$\sqrt{a}<\sqrt{100}=10$である．よって2, 3, 5, 7で割れなければaは素数である．

例
$$97 = 2\times 48+1$$
$$= 3\times 32+1$$
$$= 5\times 19+2$$
$$= 7\times 13+6$$

であるから 97 は素数である．——

100 以下の素数をすべて求めるにはどうしたらよいだろうか．1 つ 1 つを 2, 3, 5, 7 で割ってゆくのは時間がかかる．良い方法としてギリシャの数学者エラトステネス(275–194 B.C.)は数をふるい(篩)分ける，いわゆる**エラトステネスのふるい法**を考え出した．それは 100 以下の数をすべてならべ，この中でまず 2 以外の 2 の倍数をすべて消す．次に 3 以外の 3 の倍数をすべて消す．同様に 5, 7 の倍数を消す．このようにしてふるいわけたとき，あとにふるい落されずに残った数が素数である．この方法を実行すると次のようになる．

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

つまり 100 以下の素数は

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37,
41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

の 25 個である．同様に 100 以上，1000 以下の素数は

101, 103, 107, 109, 113, 127, 131, 137, 139, 149,
151, 157, 163, 167, 173, 179, 181, 191, 193, 197,
199, 211, 223, 227, 229, 233, 239, 241, 251, 257,
263, 269, 271, 277, 281, 283, 293, 307, 311, 313,

317, 331, 337, 347, 349, 353, 359, 367, 373, 379,
383, 389, 397, 401, 409, 419, 421, 431, 433, 439,
443, 449, 457, 461, 463, 467, 479, 487, 491, 499,
503, 509, 521, 523, 541, 547, 557, 563, 569, 571,
577, 587, 593, 599, 601, 607, 613, 617, 619, 631,
641, 643, 647, 653, 659, 661, 673, 677, 683, 691,
701, 709, 719, 727, 733, 739, 743, 751, 757, 761,
769, 773, 787, 797, 809, 811, 821, 823, 827, 829,
839, 853, 857, 859, 863, 877, 881, 883, 887, 907,
911, 919, 929, 937, 941, 947, 953, 967, 971, 977,
983, 991, 997

となり，結局1000以下には素数が168個ある．

§2　素因子分解の一意性

2以上のどのような合成数もいくつかの素数の積に書ける．しかもただ1通りに書ける．この事実を示すのが，この節の目標である．

自然数aを2以上の数とする．もしaが合成数ならば，aの最小の約数$p\,(>1)$は素数であり$a=pb$と書ける．もしbが合成数ならば，bの最小の約数$q\,(>1)$は素数となり，$b=qc, a=pqc$となる．以下同様にしてゆけば，aは素数の積となる．ただしaが素数のときは，素数の積という表現はおかしいけれど，便宜上このような言い方をする．aの約数を**因子**ともいう．素数である約数を**素因子**という．数を素数の積に分解することを**素因子分解**という．2以上のどのような数も素因子分解出来るわけである．

例
$$\begin{aligned}1176 &= 2\times588\\ &= 2\times2\times294\\ &= 2\times2\times2\times147\end{aligned}$$

$$= 2\times2\times2\times3\times49$$
$$= 2\times2\times2\times3\times7\times7$$
$$= 2^3\cdot3\cdot7^2. \text{ ——}$$

さて，小さな約数の順に求めて出来た素因子分解と，他の方法で出来た素因子分解が異なることがあるだろうか．たとえば1176の素因子は2と3と7となるが，この3個の素因子以外に1176の素因子はないだろうか．今まで2通りの異なった分解に出合ったことがない．だから1通りにしか素因子分解出来ないのは自明の事実である，と思っている読者も多いと思う．しかし，これは証明しなければいけないことである．証明の手段として，定理3を使う．素数pが$a\cdot b$の約数としよう．このときpの約数は1またはpであるから，$(b,p)=1$または$(b,p)=p$である．もし$(b,p)=1$ならば，定理3からaがpで割り切れる．もし$(b,p)=p$ならばpはbの約数である．よって次の補題が示された．

補題1 素数pが積$a\cdot b$の約数ならば，pはaまたはbの約数である．——

この補題を使えば，素数pがいくつかの数の積$a(b\cdot c\cdot\cdots\cdot d)$の約数のとき，$p$は$a$または$b\cdot c\cdot\cdots\cdot d$の約数である．$p$が$b(c\cdots d)$の約数ならば，$p$は$b$または$c\cdots d$の約数である．以下同様に続ければ，$p$は$a$または$b$または$c$または$\cdots d$の約数となる．つまり積のどれかの因子の約数である．このことを使い，素因子分解が1通りにしか出来ないことを示そう．

もし$a\geqq2$が2通りに素因子分解されたとしよう：

$$a = p_1p_2\cdots p_s$$
$$= q_1q_2\cdots q_t.$$

p_1は素数であり，積$q_1q_2\cdots q_t$を割るから$q_1, q_2, \cdots, q_t$のどれかを割る．もしp_1がq_1を割るとしたら，q_1は素数であることから$p_1=q_1$

となる．よって

$$p_2p_3\cdots p_s = q_2q_3\cdots q_t$$

となる．同じやり方を続ければ，$s=t$ となり素因子が同じものであることが得られる．これをまとめると次の定理の形となる．

定理 5（初等整数論の基本定理）　2以上の自然数は素数の積に分解出来る．しかもその分解の仕方はただ1通りである．——

§3　一意性が成り立たない世界

前節では，自然数の範囲では素因子分解の一意性が成り立つことを証明したが，次に示すように，一意性が成り立つのは自明でない．成り立たない世界があるのである．

2の倍数のことを**偶数**という．偶数でない数を**奇数**という．正の偶数は

$$2,\ 4,\ 6,\ 8,\ 10,\ 12,\ \cdots$$

と続いている．さて，これらの正の偶数だけの世界を考えよう．そして，今までの定義を少し変更し，この節にだけ通用する言葉を定義しよう．

3つの偶数 a, b, c が $a=b\cdot c$ となっているときにのみ，この節では a は b の倍数，b は a の約数と呼ぶことにしよう．$4=2\times2$ であるから，4は2の倍数だけれど，$6=2\times3$ において，3が奇数だから6は2の倍数ではない．このように偶数だけに制限して考えると，約数や倍数の関係は今までの定義と異なってくる．1は奇数だから偶数 a は a の約数ではない．6や10には約数が1つもない．そこで約数が1つもない偶数をこの節では素数と呼ぶことにしよう．

もし $a=b\cdot c$ となったとすると，b と c は偶数だから a は $4\cdot m$（m は自然数）という形になる．逆に $a=4\cdot m$（m は自然数）ならば $a=2(2m)$ となり，a は素数でない．つまり偶数の世界では，$4\cdot m-2$（m

は自然数)という形の数が素数となる．つまり

$$2,\ 6,\ 10,\ 14,\ 18,\ 22,\ 26,\ \cdots$$

は素数である．ところが

$$36 = 2\times18 = 6\times6$$

となり，36は2通りの仕方で素因子分解出来るわけである．

このように偶数だけの世界で，素数の定義を少し変更すると，素因子分解の一意性が成り立たないのである．このようなわけで，自然数の世界で，素因子分解の一意性が成り立つことは，あたりまえのことではなく，証明しなければいけないことなのである．

§4 素数の分布

素数は無限にあるだろうか．この問に対して“幾何学原論”は次のように明快に答えている．

もし素数が有限個しかなかったとしよう．それらを$p_1, p_2, \cdots, p_t$としよう．

$$a = p_1\cdot p_2\cdot\cdots\cdot p_t+1$$

とおく．aは素数$p_1, p_2, \cdots, p_t$のどれよりも大きいから素数でない．よってaは$p_1, p_2, \cdots, p_t$のどれかの素数で割り切れるはずである．しかし，$p_1, p_2, \cdots, p_t$のどれで割っても1余る．これは矛盾である．よって素数は無限にある．

このようにして，素数は無限にあることが示されたので，どのように大きな数xを持ってきてもxより大きな素数があることがわかった．では逆にx以下にはどのくらい素数があるだろうか．10以下には2, 3, 5, 7の4つしかない．100以下には25個ある．一般にx以下の素数の個数を$\pi(x)$で表わす．よって$\pi(10)=4$, $\pi(100)=25$である．エラトステネスのふるい法を使い，1914年D. N. レーマーは10000000以下の素数の表を作った．その後，計算機を使い1959

年 D. H. レーマーは $\pi(x)$ の次の表 3-1 を作った.

表 3-1

x	$\pi(x)$	$x/\log x$
10	4	4.3
100	25	21.7
1000	168	144.8
10000	1229	1085.7
100000	9592	8685.9
1000000	78498	72382.4
10000000	664579	620420.7
100000000	5761455	5428681.0
1000000000	50847534	48254942.4
10000000000	455052511	434294481.9

天才少年ガウスは 14 歳のころ (1791), $\pi(x)$ の変化をいろいろ調べ, $\pi(x)$ の近似値として

$$\pi(x) \doteqdot x/\log x \qquad (\log x \text{は自然対数})$$

であろうと予想した. ($y=\log x$ は自然対数である. つまり $e=2.71828\cdots$ としたとき $e^y=x$ を意味する.) 上記の表 3-1 を見ても, よい近似値であることがわかる. この予想は約 100 年後 (1896) に証明された. この定理は数学の中で最も美しい定理の 1 つと言われている. $\pi(x)$ という不規則きわまりない関数を, $x/\log x$ という非常に単純な関数で近似出来ることは驚くべきことである.

ところで素数表を眺めているといろいろなことに気付く. たとえば 4 で割り 1 余る素数をならべると

$$5,\ 13,\ 17,\ 29,\ 37,\ 41,\ 53,\ 61,\ 73,\ 89,\ 97,\ \cdots$$

となり, いくらでも続く. 3 余る素数も

$$3,\ 7,\ 11,\ 19,\ 23,\ 31,\ 43,\ 47,\ 59,\ 67,\ 71,\ 79,\ 83,\ \cdots$$

となり, いくらでも続く. ところで, 4 で割れば 3 余る素数は無限

にあることが，次のように証明される．

4で割り3余る素数が有限個しかないと仮定しよう．それらをq_1, $q_2, \cdots, q_t$とおき

$$a = 4\cdot q_1\cdot q_2\cdot\cdots\cdot q_t - 1$$

とおく．p_1, p_2を4で割れば1余る素数とする．よって$p_1=4m+1$, $p_2=4n+1$と書ける．このとき

$$\begin{aligned} p_1\cdot p_2 &= (4m+1)(4n+1) \\ &= 16mn+4m+4n+1 \\ &= 4(4mn+m+n)+1 \end{aligned}$$

であるから積も4で割れば1余る．このように4で割れば1余る数をいくつ掛けても，4で割れば1余る数しか出てこない．aは4で割ると3余る．よってaを素因子分解したとき，素因子の中には4で割れば3余る数がなければいけない．ところが4で割れば3余る素数は$q_1, q_2, \cdots, q_t$だけだと仮定したし，aをこれらで割ると割り切れないから矛盾である．すなわち，4で割れば3余る素数は無限にある．

4で割ると1余る素数も無限にある．このことは同じ論法では証明出来ないが，後に別の方法を使って証明する．もっと一般に言うと$(a, b)=1$のとき$an+b$という形をした素数が無限にあることが証明出来る(**ディリクレの素数定理**)．少し計算機を用い実験してみると，100万以下に$an+b$という形をした素数が次のように分布し

表3-2

a	b	個数	a	b	個数
3	1	39231	5	1	19617
3	2	39266	5	2	19622
4	1	39175	5	3	19665
4	3	39322	5	4	19593

ていた.

この表3-2から

$$100\text{万以下で}4\text{で割れば}1\text{余る素数の個数} = 39175$$
$$\fallingdotseq 100\text{万以下で}4\text{で割れば}3\text{余る素数の個数} = 39322$$

であることに気付く．一般の a, b に対しても，これらのことが成り立つとディリクレは証明した(1837).

さらに素数表を眺めると

3 と 5，5 と 7，11 と 13，17 と 19，29 と 31，…

というように p と $p+2$ が共に素数である組合せがたくさん見つかる．このような組み合わさった素数を**双子素数**という．計算機を使い，303 桁の双子素数が見つかっている．ところで双子素数は無限にあるだろうか．これは未解決な問題である.

ところで或る素数 p に対して，次の素数(p より大きい最小の素数)はどのくらい大きいだろうか．この問に対して，次の素数は $2p$ より小さいことがわかっている(チェビシェフの定理，1852)．たとえば

$$2 < 3 < 4$$
$$3 < 5 < 6$$
$$5 < 7 < 10$$
$$7 < 11 < 14$$
$$11 < 13 < 22$$

となる．単純な定理だけれど，証明はむずかしい．後に p と p^2 の間には素数があることを証明しよう.

ゴールドバッハからオイラーへの手紙(1742)の中に奇妙な予想がある．それは 4 以上の偶数はすべて 2 つの素数の和であろう，という推測である(**ゴールドバッハの予想**)．たとえば

$$4 = 2+2$$

$$6 = 3+3$$
$$8 = 3+5$$
$$10 = 3+7 = 5+5$$
$$12 = 5+7$$

となり，小さい数で調べる限り，いつも正しい．しかしこの予想もまだ証明されていない．

ともかく，素数の分布に関しては未解決な問題がたくさんある．

§5 最大の素数

素数は無限にあるから最大の素数というものはない．しかし現在(1981)具体的に知られている素数の中で最大な数は定まっている．それは

$$M_{44497} = 2^{44497}-1 \qquad (44497\text{ は素数})$$

という数である．この数の常用対数を取ってみると

$$\begin{aligned}\log_{10}M_{44497} &\fallingdotseq \log_{10}2^{44497}\\ &= 44497\times\log_{10}2\\ &\fallingdotseq 44497\times 0.30103\\ &\fallingdotseq 13394.9\end{aligned}$$

となるので M_{44497} は13395桁の素数である．何故このように大きな数が素数だと判定出来るのだろうか．勿論，世界最高速の計算機を長時間使って得た結果ではあるが，小さい順に $\sqrt{M_{44497}}$ まで割っていったわけではない．小さい順に割っていったのでは，宇宙が出来てから今まで最高速の計算機を使いつづけたとしても，素数だと判定出来ない．このことについて少し説明しよう．

一般に p を素数とするとき

$$M_p = 2^p-1$$

となる数を考える．少し計算すると

$2^2-1=3=$ 素数

$2^3-1=7=$ 素数

$2^5-1=31=$ 素数

$2^7-1=127=$ 素数

$2^{11}-1=2047=23\times 89$　(中世に知られていた)

$2^{13}-1=8191=$ 素数　(中世に知られていた)

$2^{17}-1=131071=$ 素数　(Cataldi, 1588)

$2^{19}-1=524287=$ 素数　(Cataldi, 1588)

となる．始めの4つはギリシャ時代に素数だと知られていた．1000以上の数はギリシャ時代には非常に大きな数と思われていたのであろう．だから1000以上の数に対して割り算を実行するのは，とんでもないことだと思ったにちがいない．

ともかく p が素数でも 2^p-1 が素数とはかぎらない．2^p-1 が素数になるとき，それは**メルセンヌ数**と呼ばれている．現在知られているメルセンヌ数は27個あり，p が

2, 3, 5, 7, 13, 17, 19, 31, 61, 87, 107, 127,
521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689,
9941, 11213, 19937, 21701, 23209, 44497

のときである．

$p=31$ のとき $2^{31}-1$ が素数であることは，オイラーが1772年，小さい順に割り算を実行して確かめた．それ以後の4つに対しては，ルカスが1876年ルカステストという，非常に能率的な計算法を考え出して確かめた．

ルカステストとは

$$S_1=4$$

$$S_2={S_1}^2-2$$

$$S_3={S_2}^2-2$$

$$S_4 = {S_3}^2 - 2$$
$$\vdots$$

と計算していくとき，p が素数のとき

$$M_p = 2^p - 1 = \text{素数} \Longleftrightarrow S_{p-1} \text{ が } M_p \text{ で割り切れる}$$

という判定法である．S_{p-1} が M_p で割り切れるか否かが問題なので，$S_2, S_3, \cdots$ を計算していく途中で S_i が M_p より大きくなれば，S_i を M_p で割った余りにおきかえてよい．電子計算機の中では数は2進法で表わされているので $S_i = 2^p \cdot A + B$ のとき

$$\begin{aligned} S_i &= (2^p - 1)A + A + B \\ &= M_p \cdot A + (A + B) \end{aligned}$$

となり，実質的には割り算は必要でない．よって $p-2$ 回の M_p 以下の数の掛け算で素数か否か判定出来るわけである．$\sqrt{2^p-1}$ までの数で割っていくのとは桁違いに能率的な判定法である．とはいうものの p が127より大きいと，筆算および手廻し計算機ではとても不可能な計算である．p が127より大きい場合の結果はすべて電子計算機を使って確かめられた．

§6　フェルマー数

フェルマー(1601–1665)は $n \geqq 0$ に対して

$$F_n = 2^{2^n} + 1 \qquad (n = 0, 1, 2, \cdots)$$

は素数であろうと予想した．事実

$$\begin{aligned} F_0 &= 2^1 + 1 = 3, & F_3 &= 2^8 + 1 = 257 \\ F_1 &= 2^2 + 1 = 5, & F_4 &= 2^{16} + 1 = 65537 \\ F_2 &= 2^4 + 1 = 17 \end{aligned}$$

は素数である．F_n が素数のとき，**フェルマー数**という．フェルマー数は上記のように5つ続いたけれど，フェルマーの予想に反して

$$F_5 = 2^{32} + 1 = 4294967297 = 641 \times 6700417$$

となることをオイラー(1732)が示した．F_6 に関してはランドリー(1880)が 82 歳のとき，毎日数時間ずつ計算して数か月かけて

$$F_6 = 2^{64}+1 = 274177\times 67280421310721$$

と分解出来ることを見つけた．F_7 に関しては

$$F_7 = 2^{128}+1$$
$$= 59649589127417217\times 5704689200685129054721$$

と分解出来ることが計算機を使い確かめられている(1970)．F_8 も

$$F_8 = (604944512477\times 2^{11}+1)\times(45635566267264637582599393652151804972681268330878021767715\times 2^{11}+1)$$

と分解出来ることが最近(1980)確かめられた．$n=9, 10, \cdots, 19$ に対しても，F_n は合成数であることがわかっている．しかし，たとえば F_{14} に関しては素因子が 1 つも見つかっていない．素因子が見つからないのに何故合成数だと判定出来るのだろうか．実はルカステストと同じように Pepin の判定法

$$F_n = \text{素数} \Longleftrightarrow 3^{(F_n-1)/2}+1 \text{ が } F_n \text{ の倍数}$$

という方法がある．この判定法において，掛け算が何回必要かというと，$(F_n-1)/2=2^{2^n-1}$ 回必要なわけではない．$n=14$ のとき，$(F_{14}-1)/2=2^{16383}$ となるが，

$$3^2 = 3\cdot 3,\ \ 3^4 = 3^2\cdot 3^2,\ \ 3^8 = 3^4\cdot 3^4,\ \ \cdots$$

と計算していけば，16383 回で $3^{(F_{14}-1)/2}$ が計算出来る．このような事情により，素数か否かだけは能率良く判定されるわけである．

このようにしていろいろの n に対して調べてみると，フェルマーの予想とは正反対に $n\geqq 5$ のとき，素数は 1 つも見つかっていない．

F_n にはいろいろな性質がある．ここでは $m<n$ ならば F_m と F_n は互いに素，つまり $(F_m, F_n)=1$ であることを示そう．

$m+k=n$ $(k>0)$ とすると，F_n の定義から

$$F_n-2 = (2^{2^m})^{2^k}-1$$

となる．$2^{2^m}=a, 2^k=l$ とおくと，l は偶数なので

$$
\begin{aligned}
F_n-2 &= a^l-1 \\
&= (a+1)(a^{l-1}-a^{l-2}+\cdots+a-1) \\
&= F_m\cdot(a^{l-1}-a^{l-2}+\cdots+a-1)
\end{aligned}
$$

となる．この式から F_n と F_m の公約数 d は2の約数となる．ところが，F_n も F_m も奇数であるから，$d=1$ とならざるを得ない．よって$(F_m, F_n)=1$ が示された．

この事実から，$F_n (n=0, 1, 2, \cdots)$ を素因子分解すると，2つ以上の F_n に共通する素因子はない．すなわち $F_0, F_1, \cdots, F_n$ までには少なくとも $n+1$ 個の素数が素因子として現われる．よって素数が無限にあることの別証明が得られた．また，素数を小さい順に並べたとき，n 番目の素数 p_n より大きい素数が $F_0, F_1, \cdots, F_n$ のどれかの素因子となっているから $p_n<F_n$, つまり

$$p_n < 2^{2^n}+1$$

が得られたわけである．ただし，チェビシェフの定理を認めれば $p_n<p_{n+1}<2p_n$ であるから，もっとよい不等式

$$p_n \leqq 2^n$$

が得られる．

さて，青年ガウスが18歳のとき(1796)，定木とコンパスで正17角形を作図した．このとき，ギリシャ時代を真に越える幾何学が現われた，と言ってよい．ガウスはフェルマー数 F_n に対して正 F_n 角形が作図出来ることも示した．よって，原理的には正257角形や正65537角形も定木とコンパスだけで作図出来る．逆に p が素数のとき，もし正 p 角形が作図出来るとしたら，p はフェルマー数でなければならない(ガウス)．よって正7角形などは，定木とコンパスだけでは作図出来ない．

第4章　約数と倍数

§1　約数の個数

まず，トランプの札を1からKまで並べてみよう．

1　2　3　4　5　6　7　8　9　10　J　Q　K

次に偶数番目にある札を裏返しにしよう．

1　*　3　*　5　*　7　*　9　*　J　*　K

さらに3番目ずつ裏返しにしてみよう．

1　*　*　*　5　6　7　*　*　*　J　Q　K

6やQはふたたび裏返されたので表となった．次に4番目ずつ裏返しにしよう．

1　*　*　4　5　6　7　8　*　*　J　*　K

同じように5番目ごと，6番目ごと，7番目ごと，…，13番目ごとと裏返しにしていくと，次のように変化する．

1　*　*　4　*　6　7　8　*　10　J　*　K
1　*　*　4　*　*　7　8　*　10　J　Q　K
1　*　*　4　*　*　*　8　*　10　J　Q　K
1　*　*　4　*　*　*　*　*　10　J　Q　K
1　*　*　4　*　*　*　*　9　10　J　Q　K
1　*　*　4　*　*　*　*　9　*　J　Q　K
1　*　*　4　*　*　*　*　9　*　*　Q　K
1　*　*　4　*　*　*　*　9　*　*　*　K
1　*　*　4　*　*　*　*　9　*　*　*　*

さて，最後に表になった札は何かと見ると，1と4と9の3枚だ

けである．この3つの数に共通している性質は，$1=1^2, 4=2^2, 9=3^2$ となること，すなわち**平方数**であることに気付く．何故であろうか．

偶数番目にひっくり返される札は，2の倍数である．3番目ずつにひっくり返される札は3の倍数である．以下同様に考えれば，最後に表になっている札とは，偶数回ひっくり返される札である．つまり，その札の1以外の約数の個数が偶数個の場合である．言いかえれば，すべての約数の個数が奇数の場合である．次に平方数のみが約数の個数が奇数であることを示そう．

自然数 a を素因子分解して

$$a = p_1 \cdot p_2 \cdot \cdots \cdot p_t$$

となったとしよう．$p_1, \cdots, p_t$ の中に同じ素数があるときは，まとめてあらためて書き直し

$$a = {p_1}^{e_1} \cdot {p_2}^{e_2} \cdot \cdots \cdot {p_s}^{e_s} \qquad (1 \leqq e_i)$$

と表わそう．この形を a の**標準分解**という．また e_i を素数 p_i の**指数**という．b を a の約数とし，$a=b \cdot c$ とする．b と c を標準分解して

$$b = {q_1}^{f_1} \cdot {q_2}^{f_2} \cdot \cdots \cdot {q_t}^{f_t}$$
$$c = {r_1}^{g_1} \cdot {r_2}^{g_2} \cdot \cdots \cdot {r_u}^{g_u}$$

となったとすると

$$b \cdot c = {q_1}^{f_1} \cdot \cdots \cdot {q_t}^{f_t} \cdot {r_1}^{g_1} \cdot \cdots \cdot {r_u}^{g_u}$$
$$= {p_1}^{e_1} \cdot \cdots \cdot {p_s}^{e_s}$$

となっている．つまり ${q_1}^{f_1} \cdot \cdots \cdot {q_t}^{f_t} \cdot {r_1}^{g_1} \cdot \cdots \cdot {r_u}^{g_u}$ をまとめ直せば，素因子分解の一意性から ${p_1}^{e_1} \cdot \cdots \cdot {p_s}^{e_s}$ となる．よって，$q_1, \cdots, q_t$ は $p_1, \cdots, p_s$ のどれかでなければならず，たとえば $q_1=p_1$ のときは $f_1 \leqq e_1$ でなければならない．b の素因子として $p_1, \cdots, p_s$ のすべてが現われるわけではないけれど，現われないときは $p^0=1$ という規約を用いて，指数が0だと思えばよい．つまり，b を素因子分解すれば次の

形となる．

$$b = p_1^{f_1} \cdot p_2^{f_2} \cdot \cdots \cdot p_s^{f_s} \qquad (0 \leqq f_i \leqq e_i).$$

さて，素因子分解の一意性のおかげで $f_1, \cdots, f_s$ の組合せが変われば値も変わる．f_1 は0から e_1 まで $1+e_1$ 通り動くことが出来る．同様に考えていくと，$f_1, \cdots, f_s$ の組合せ数，つまり a の約数の個数 $T(a)$ は

$$T(a) = (1+e_1)(1+e_2)\cdots(1+e_s)$$

となる．この中には $f_1=f_2=\cdots=f_s=0$ となる約数1も $f_1=e_1, f_2=e_2, \cdots, f_s=e_s$ となる約数 a も数えられている．

例　$28=2^2\cdot 7$．よって28の約数は

$$2^0\cdot 7^0 = 1,\ 2^1\cdot 7^0 = 2,\ 2^2\cdot 7^0 = 4$$
$$2^0\cdot 7^1 = 7,\ 2^1\cdot 7^1 = 14,\ 2^2\cdot 7^1 = 28$$

の $(1+2)(1+1)=6$ 通りである．——

さて，$1+e_1, 1+e_2, \cdots, 1+e_s$ のどれかが偶数だと $T(a)$ は2で割れてしまう．よって $T(a)$ が奇数であるためには $e_1, e_2, \cdots, e_s$ すべてが偶数であることが必要十分である．$e_1, \cdots, e_s$ が偶数ならば $e_i=2\cdot f_i$ と書けば

$$\begin{aligned} a &= p_1^{2f_1} \cdot p_2^{2f_2} \cdot \cdots \cdot p_s^{2f_s} \\ &= (p_1^{f_1} \cdot p_2^{f_2} \cdot \cdots \cdot p_s^{f_s})^2 \end{aligned}$$

となり，a は平方数となる．逆に a が平方数ならば，a は b^2 と書かれ，b を標準分解すると

$$\begin{aligned} a &= b^2 \\ &= (p_1^{f_1} \cdot \cdots \cdot p_s^{f_s})^2 \\ &= p_1^{2f_1} \cdot \cdots \cdot p_s^{2f_s} \end{aligned}$$

となり，指数はすべて偶数となる．以上でトランプの謎は明らかになった．

§2　約数の和

自然数 a の素因子分解がわかれば，その約数の形が定まるので，a のすべての約数の和 $S(a)$ も計算出来る．

(1)
$$a = p_1^{e_1}\cdot p_2^{e_2}\cdot\cdots\cdot p_s^{e_s}$$

とすれば，a の約数は

(2)
$$p_1^{f_1}\cdot p_2^{f_2}\cdot\cdots\cdot p_s^{f_s},\quad 0\leqq f_i\leqq e_i,\ 1\leqq i\leqq s$$

となる．まず $s=1$ の場合を考えてみよう．$a=p^e$ とすれば，a のすべての約数は

$$1,\ p,\ p^2,\ \cdots,\ p^e$$

となるので，等比数列の和の公式を使い

$$S(a) = 1+p+p^2+\cdots+p^e = \frac{p^{e+1}-1}{p-1}$$

となる．$s=2$ の場合，$a=p^e\cdot q^f$ とすれば

$$\begin{aligned}S(a) &= 1+p+p^2+\cdots+p^e\\ &\quad +q+p\cdot q+p^2\cdot q+\cdots+p^e\cdot q\\ &\quad +\cdots \qquad\qquad \cdots+p^e\cdot q^{f-1}\\ &\quad +q^f+p\cdot q^f+p^2\cdot q^f+\cdots+p^e\cdot q^f\\ &= (1+p+\cdots+p^e)(1+q+\cdots+q^f)\\ &= S(p^e)\cdot S(q^f)\\ &= \frac{p^{e+1}-1}{p-1}\cdot\frac{q^{f+1}-1}{q-1}\end{aligned}$$

となる．同様に

(3)
$$S(p_1^{e_1}\cdot p_2^{e_2}\cdot\cdots\cdot p_s^{e_s}) = S(p_1^{e_1})\cdot S(p_2^{e_2})\cdot\cdots\cdot S(p_s^{e_s})$$

となる．何故ならば

$$(1+p_1+\cdots+p_1^{e_1})(1+p_2+\cdots+p_2^{e_2})\cdots(1+p_s+\cdots+p_s^{e_s})$$

をばらばらにしてみれば，(2)の形の数が1通りずつすべて現われるからである．

例　$28=2^2\cdot 7$ の約数の和は

$$S(28)=(1+2+2^2)(1+7)=7\times 8=56=28\times 2.$$ ——

さて，(3)の形から a と b が互いに素ならば

$$S(a\cdot b)=S(a)\cdot S(b)$$

となることがわかる．何故ならば，a, b を

$$a={p_1}^{e_1}\cdots {p_s}^{e_s}$$
$$b={q_1}^{f_1}\cdots {q_r}^{f_r}$$

と標準分解すると，互いに素であることから

$$a\cdot b={p_1}^{e_1}\cdots {p_s}^{e_s}\cdot {q_1}^{f_1}\cdots {q_r}^{f_r}$$

が積の標準分解となり

$$\begin{aligned} S(a\cdot b) &= S({p_1}^{e_1})\cdot\cdots\cdot S({p_s}^{e_s})\cdot S({q_1}^{f_1})\cdot\cdots\cdot S({q_r}^{f_r}) \\ &= S(a)\cdot S(b) \end{aligned}$$

となるからである．

§3　完全数

自然数 a の約数のうち，a 以外の約数を加え合せると a になることがある．たとえば $a=6$ のとき，約数は $1, 2, 3, 6$ と4個あるけれど，6以外の約数の和は $1+2+3=6$ となる．このようなとき，a を**完全数**という．a 自身も加えれば $S(a)=2a$ となるとき，a を完全数というわけである．28も完全数である．

例　$p=$素数，$q=2^p-1=$素数 のとき，つまり q がメルセンヌ数のとき $a=2^{p-1}\cdot q$ とおくと

$$S(a)=S(2^{p-1})\cdot S(q)$$

$$S(2^{p-1})=1+2+2^2+\cdots+2^{p-1}=\frac{2^p-1}{2-1}$$

$$S(q) = 1+q$$

であるから

$$S(a) = \frac{2^p-1}{2-1}\cdot(1+q)$$
$$= (2^p-1)\cdot 2^p$$
$$= 2\cdot a.$$

よって a は完全数である. ——

例 a が偶数の完全数とすると, $a=2^{p-1}\cdot q$, $p=$素数, $q=2^p-1$ =素数 となる(オイラー).

なぜならば

$$a = 2^{e-1}\cdot b \qquad (b=\text{奇数},\ e\geqq 2)$$

とすると, $(2^{e-1}, b)=1$ から

$$S(a) = S(2^{e-1})\cdot S(b)$$
$$= \frac{2^e-1}{2-1}\cdot S(b)$$
$$= (2^e-1)\cdot S(b)$$

となる. 他方, $a=$完全数であることから

$$S(a) = 2a$$
$$= 2^e\cdot b$$
$$= (2^e-1)b+b$$

となる.

$$\therefore\quad (2^e-1)\cdot S(b) = (2^e-1)b+b.$$

両辺を 2^e-1 で割れば

(1) $$S(b) = b+\frac{b}{2^e-1}$$

となる. 左辺は整数であるから, 右辺も整数となり, 特に $\frac{b}{2^e-1}$ も整数となる. つまり, 2^e-1 は b の約数であり, 1とも異なるので

$\dfrac{b}{2^e-1}$ は b より小さな b の約数である．(1)は b のすべての約数の和が，b の2つの約数である b と $\dfrac{b}{2^e-1}$ の和で終っていること，つまり，b には2つしか約数がないことを示している．よって b は素数となり $S(b)=b+1$ となる．よって $\dfrac{b}{2^e-1}=1$ となり $b=2^e-1$ が得られた．さて $2^e-1=b$ が素数となるためには e が素数でなければならない．なぜなら，もし e が合成数ならば $e=k\cdot l$, $2^k=c$, $1<k$, $1<l$ とおけば

$$
\begin{aligned}
2^e-1 &= 2^{kl}-1 \\
&= c^l-1 \\
&= (c-1)(c^{l-1}+c^{l-2}+\cdots+c+1)
\end{aligned}
$$

となり，素数でなくなる．よって $e=p=$素数 とおけば，$b=2^p-1=$素数 となり，$a=2^{p-1}\cdot(2^p-1)$ が得られた．——

以上2つの例から，偶数の完全数はメルセンヌ数と同じ数だけあることがわかった．よって，現在のところ27組見つかっている．偶数の完全数が無限にあるか否かは，未解決の問題である．奇数の完全数は1つも見つかっていない．計算機を使い，10^{50} 以下には奇数の完全数が存在しないことは確かめられているが，10^{50} 以上に奇数の完全数が存在するか否かは未解決である．

§4　最大公約数と最小公倍数

2つ以上の数の共通の約数を公約数といい，その中で最大な数を**最大公約数**(greatest common divisor)という．

$a, b, \cdots, e$ の最大公約数を記号で

$$\text{G.C.D.}\{a, b, \cdots, e\} \quad \text{または} \quad (a, b, \cdots, e)$$

と書く．

3つの数 a, b, c のどれかを割る素数を $p_1, p_2, \cdots, p_r$ とし，a, b, c を

標準分解して

(1) $$a = p_1{}^{e_1}\cdot p_2{}^{e_2}\cdot\cdots\cdot p_r{}^{e_r} \qquad (0\leqq e_i)$$

(2) $$b = p_1{}^{f_1}\cdot p_2{}^{f_2}\cdot\cdots\cdot p_r{}^{f_r} \qquad (0\leqq f_i)$$

(3) $$c = p_1{}^{g_1}\cdot p_2{}^{g_2}\cdot\cdots\cdot p_r{}^{g_r} \qquad (0\leqq g_i)$$

となったとする．このとき $d=(a, b, c)$ とすると，d を割る素数は $p_1, p_2, \cdots, p_r$ 以外にはないので

$$d = p_1{}^{h_1}\cdot p_2{}^{h_2}\cdot\cdots\cdot p_r{}^{h_r} \qquad (0\leqq h_i)$$

と書ける．ところで，d は a, b, c の公約数であるから

(4) $$h_i \leqq e_i, \quad h_i \leqq f_i, \quad h_i \leqq g_i \qquad (1\leqq i\leqq r)$$

でなければならない．公約数の中で最大になるようにするには(4)の条件の下で h_i を出来るだけ大きくすればよい．つまり e_i, f_i, g_i のうちの最小な数を h_i とすればよい．記号で

$$h_i = \min\{e_i, f_i, g_i\} = e_i, f_i, g_i \text{ のうちの最小な数}$$

となる．

例
$$a = 2^3\cdot 3^2\cdot 5^2 = 1800$$
$$b = 2^0\cdot 3^3\cdot 5^3 = 3375$$
$$c = 2^2\cdot 3^4\cdot 5 \ = 1620$$

のとき $(a, b, c)=2^0\cdot 3^2\cdot 5 = 45$. ——

このように素因子分解出来れば最大公約数は求まる．しかし，ユークリッドの互除法を次のように用いれば，素因子分解の必要はない．

3つの数 e_i, f_i, g_i の最小な数とは，e_i と f_i の小さい方の数と g_i を比べ，小さい方を求めればよい．つまり

$$\min\{e_i, f_i, g_i\} = \min\{\min\{e_i, f_i\}, g_i\}$$

となる．この式は

$$(a, b, c) = ((a, b), c)$$

を意味している．よって，互除法を2回用いればよい．

例　　$a = 1800,\quad b = 3375,\quad c = 1620$

のとき

$$3375 = 1800 \times 1 + 1575$$
$$1800 = 1575 \times 1 + 225$$
$$1575 = 225 \times 7 + 0$$

となり，$(a, b) = 225$ が得られる．次に

$$1620 = 225 \times 7 + 45$$
$$225 = 45 \times 5 + 0$$

から $(225, c) = 45$ が得られた．——

2つ以上の数の共通の倍数を公倍数といい，その中で最小の数を**最小公倍数**(least common multiple)という．

$a, b, \cdots, e$ の最小公倍数を記号で

$$\mathrm{L.C.M.}\{a, b, \cdots, e\}$$

と書く．

a, b, c が(1),(2),(3)のように標準分解しているとき，$m = \mathrm{L.C.M.}\{a, b, c\}$ を求めるには最大公約数を求める考え方と同様にして

$$m = p_1{}^{k_1} \cdot p_2{}^{k_2} \cdot \cdots \cdot p_r{}^{k_r},$$

$k_i = \max\{e_i, f_i, g_i\} = e_i, f_i, g_i$ のうちの最大な数とすればよい．また

$$\max\{e_i, f_i, g_i\} = \max\{\max\{e_i, f_i\}, g_i\}$$

を用いると

$$\mathrm{L.C.M.}\{a, b, c\} = \mathrm{L.C.M.}\{\mathrm{L.C.M.}\{a, b\}, c\}$$

となる．$\mathrm{L.C.M.}\{a, b\} = a \cdot b/(a, b)$ であるから最小公倍数も互除法から計算出来る．

例　　$a = 1800,\quad b = 3375,\quad c = 1620$

のとき，標準分解から

$$\mathrm{L.C.M.}\{a, b, c\} = 2^3 \cdot 3^4 \cdot 5^3 = 81000$$

となる.

標準分解を利用しないときは，まず

$$\begin{aligned}\text{L.C.M.}\{a, b\} &= a\cdot b/(a, b)\\ &= 1800\cdot 3375/225\\ &= 27000\end{aligned}$$

となり

$$\begin{aligned}27000 &= 1620\times 16+1080\\ 1620 &= 1080\times 1+540\\ 1080 &= 540\times 2+0\end{aligned}$$

から $(27000, c)=540$ が得られ

$$\begin{aligned}\text{L.C.M.}\{27000, c\} &= 27000\times 1620/540\\ &= 81000\end{aligned}$$

が得られる. ——

以上のように，約数，倍数に関して標準分解を用いると，理論的にはとても見通しがよくなる.

§5　ピタゴラスの定理

直角三角形の斜辺の上に立つ正方形の面積は，他の2辺の上に立つ正方形の面積の和に等しい，というのが**ピタゴラスの定理**である. 式で書くと，3辺の長さを a, b, c とすれば $a^2+b^2=c^2$ ということである. ここで a, b, c すべてが自然数になることがある. たとえば，

$$3^2+4^2 = 9+16 = 25 = 5^2$$

$$5^2+12^2 = 25+144 = 169 = 13^2$$

となる. 他に a, b, c が自然数になる場合がどのくらいあるだろうか. 1組の解 a, b, c があれば，それらを同時に m 倍しても解であるから，a, b, c には共通の約数がない場合を考えよう. つまり $(a, b, c)=1$ の場合のみを考えるわけである. $(a, b)=d$ とすれば，$a=d\cdot a_1$, $b=d\cdot$

b_1 となり $c^2=a^2+b^2=d^2(a_1{}^2+b_1{}^2)$ から，d は c の約数となる．つまり d は a, b, c の公約数となる．$(a, b, c)=1$ であるから $d=1$ でなければならない．つまり $(a, b)=1$ となる．同様に $(a, c)=1, (b, c)=1$ となる．

さて，偶数 $2x$ を自乗すれば $(2x)^2=4x^2$ となり 4 で割り切れる．奇数 $2x+1$ を自乗すれば

$$(2x+1)^2 = 4x^2+4x+1 = 4(x^2+x)+1$$

となり 4 で割れば 1 余る．もし a, b 共に奇数だとすると，$a^2=4m+1, b^2=4n+1$ と書け

$$c^2 = a^2+b^2 = 4(m+n)+2$$

となる．c^2 は 4 で割ると 0 または 1 しか余らないから矛盾である．よって a または b は偶数である．ただし $(a, b)=1$ であるから片方は奇数である．そこで，a=偶数，b=奇数とする．このとき $a^2=4m$, $b^2=4n+1$ とおけば

$$c^2 = a^2+b^2 = 4(m+n)+1$$

から c は奇数でなければならない．このとき

$$\left(\frac{a}{2}\right)^2 = \frac{c^2-b^2}{4} = \frac{c+b}{2}\cdot\frac{c-b}{2}$$

と変形し，$(c+b)/2=x, (c-b)/2=y$ とおくと，b, c 共に奇数であることから，x, y は自然数となる．$d=(x, y)$ とおくと，$x+y=c, x-y=b$ から d は c と b の公約数となる．$(c, b)=1$ から $d=1$ となる．つまり x と y は互いに素になる．しかも

$$(a/2)^2 = x\cdot y, \qquad (x, y) = 1$$

であるから，x, y を素因子分解してみればわかるように，x および y は共に平方数でなければならない．つまり $x=u^2, y=v^2$ となる自然数 u, v が存在する．まとめると

$$\frac{c+b}{2}=x=u^2, \qquad \frac{c-b}{2}=y=v^2, \qquad \left(\frac{a}{2}\right)^2=u^2\cdot v^2.$$

よって$(x, y)=1$に注意すれば

$$a=2uv, \qquad b=u^2-v^2, \qquad c=u^2+v^2,$$
$$u>v, \qquad (u, v)=1$$

が得られる．またu, v共に奇数だと，b, cが共に偶数になってしまうので，片方は偶数，片方は奇数である．

逆に2つの自然数u, vが片方は偶数で，しかも

$$u>v, \qquad (u, v)=1$$

が成り立つならば

$$a=2uv, \qquad b=u^2-v^2, \qquad c=u^2+v^2$$

とおくことにより

$$\begin{aligned} a^2+b^2 &= (2uv)^2+(u^2-v^2)^2 \\ &= 4u^2v^2+u^4-2u^2v^2+v^4 \\ &= u^4+2u^2v^2+v^4 \\ &= (u^2+v^2)^2 \\ &= c^2 \end{aligned}$$

となる．さらにu, vの片方だけが偶数であることから，b, c共に奇数となり，$(b, c)=d$とおくとdは奇数となり

$$c+b=2u^2, \qquad c-b=2v^2$$

からdはu^2, v^2の公約数である．dの素因子の1つをpとすれば，pはu^2, v^2の公約数となり，よってpはu, vの公約数となる．しかし$(u, v)=1$であることから$d=1$でなければいけない．よって$(a, b, c)=1$が得られた．まとめると次のようになる．

定理6　$a^2+b^2=c^2$の自然数解のうち，$(a, b, c)=1$となるものは

$$u>v, \qquad (u, v)=1, \qquad u, v\text{の片方は偶数}$$

となる自然数u, vにより

$$a=2uv, \quad b=u^2-v^2, \quad c=u^2+v^2$$

と書き表わすことが出来る．またこのように書き表わされたものはすべて $a^2+b^2=c^2$, $(a, b, c)=1$ を満たす．——

例　$u, v, a^2+b^2=c^2$ の表を作ってみよう．

表 4-1

u	v	$a^2+b^2=c^2$	u	v	$a^2+b^2=c^2$
2	1	$4^2+3^2=5^2$	7	2	$28^2+45^2=53^2$
4	1	$8^2+15^2=17^2$	4	3	$24^2+7^2=25^2$
6	1	$12^2+35^2=37^2$	8	3	$48^2+55^2=73^2$
3	2	$12^2+5^2=13^2$	10	3	$60^2+91^2=109^2$
5	2	$20^2+21^2=29^2$			

§6 フェルマーの大定理

ピタゴラスの定理を調べているとき，フェルマーは

(1) $$x^3+y^3=z^3$$

(2) $$x^4+y^4=z^4$$

などは自然数解はないであろうと予想した(1638年ごろ)．もっと正確に言えば，もし n が3以上ならば

(3) $$x^n+y^n=z^n \qquad (n\geqq 3)$$

は自然数解を持たないだろう，という予想である．ピタゴラスの定理などさまざまな不定方程式を研究したギリシャの数学者ディオファントスが書いた本があるが，フェルマーはこの本のラテン語訳を発行したとき，手控本の余白に

“私は真に驚くべき証明を発見したが，その証明を書くには，この余白はせますぎる”

と書きのこした．しかし，現在にいたるまで証明されていないところをみると，何か思い違いをしたのであろう．後にフェルマー自身

は $n=4$ の場合には解がないことを証明している．ともかく，一般の場合には証明されていないが，フェルマーが正しいと明言したので，この予想は**フェルマーの大定理**と呼ばれている．

$n=4$ の場合，つまり(2)は自然数解を持たないことを証明しよう．

もし(2)に解があるならば，z^2 を新しく z とおけば

$$(4) \qquad x^4+y^4 = z^2$$

に自然数解がある．(4)の自然数解のうち，z の値が最小となるものを1つ固定する．このとき $(x, y, z)=d$ とおくと，$d=1$ である．なぜなら，もし $d>1$ とし，$x=dx_1, y=dy_1$ とおくと，(4)の左辺は $d^4(x_1{}^4+y_1{}^4)$ となる．よって右辺が d^4 で割れる．つまり z が d^2 で割れ $z=d^2\cdot z_1$ となる．このとき

$$x_1{}^4+y_1{}^4 = z_1{}^2 \qquad (z_1<z)$$

となり z の最小性に反する．よって $(x, y, z)=1$ となる．

さて，(4)を書き直すと

$$(5) \qquad (x^2)^2+(y^2)^2 = z^2, \qquad (x^2, y^2, z) = 1$$

となる．よって，前節の定理6を使うと，x^2 または y^2 が偶数となり，かりに x^2 が偶数だとすると

$$x^2 = 2uv, \qquad y^2 = u^2-v^2, \qquad z = u^2+v^2$$

$$u > v, \qquad (u, v) = 1, \qquad u, v \text{ の片方は偶数}$$

となる u, v が存在する．

もし $u=$偶数，$v=$奇数 とすると，$u=2m, v=2n+1$ と書けて

$$\begin{aligned} y^2 &= u^2-v^2 \\ &= (2m)^2-(2n+1)^2 \\ &= 4m^2-4n^2-4n-1 \\ &= 4(m^2-n^2-n-1)+3 \end{aligned}$$

となり，y^2 を4で割ると3余る．y は奇数であるが，$y=2k+1$ とおくと

$$y^2 = (2k+1)^2$$
$$= 4k^2+4k+1$$
$$= 4(k^2+k)+1$$

となり，4で割れば1余る．これは4で割れば3余ることと矛盾する．よって u=奇数，v=偶数 となる．

x^2 が偶数であるから x は偶数となり

$$(x/2)^2 = u\cdot(v/2)$$

と書ける．$(u, v)=1$ であるから当然 $(u, v/2)=1$ となる．互いに素な数の積が平方数であることは，おのおのが平方数であることを意味する．よって

$$u = {z_1}^2, \qquad v/2 = w^2$$

となる自然数 z_1, w が存在する．このとき

$$y^2 = u^2-v^2$$
$$= {z_1}^4-4w^4$$

となる．w^4 を書き直すと

$$(6) \qquad w^4 = ({z_1}^4-y^2)/4$$
$$= \frac{{z_1}^2+y}{2}\cdot\frac{{z_1}^2-y}{2}$$

となる．$y, {z_1}^2=u$ は共に奇数であるから

$$u_1 = ({z_1}^2+y)/2, \qquad v_1 = ({z_1}^2-y)/2$$

は共に自然数である．次に $(u_1, v_1)=1$ を示そう．

もし $(u_1, v_1)=d>1$ とすると，

$$u_1+v_1 = {z_1}^2 = u$$
$$u_1-v_1 = y$$

から d は u と y の公約数となる．また

$$v^2 = u^2-y^2$$

であるから d は v^2 の約数となる．d の素因子の1つを p とすれば，

p は v^2 の約数であるから p は v の約数である．よって p は u と v の公約数となり $(u, v)=1$ に反する．つまり $(u_1, v_1)=1$ となる．

さて(6)から

$$w^4 = u_1 \cdot v_1, \qquad (u_1, v_1) = 1$$

となる．互いに素な数の積が4乗数になるためには，素因子分解してみれば，おのおのが4乗数でなければならないことがわかる．よって

$$u_1 = {x_1}^4, \qquad v_1 = {y_1}^4$$

となる．このとき

$$ {x_1}^4 + {y_1}^4 = u_1 + v_1 = {z_1}^2 $$
$$ {z_1}^2 = u < u^2 + v^2 = z < z^2 $$

となり，x_1, y_1, z_1 は(4)を満たし，しかも $z_1 < z$ となる．これは z の最小性に反する．この矛盾は(4)に自然数解があると仮定したから生じた．よって(4)には自然数解がない．したがって(2)にも自然数解がない．よって $n=4$ の場合，フェルマーの大定理は正しい．

n が4の倍数のとき，つまり $n=4m$ と表わせるとき，もし(3)に解があれば

$$x^{4m} + y^{4m} = z^{4m}$$
$$(x^m)^4 + (y^m)^4 = (z^m)^4$$

となり，$n=4$ のとき解があることになる．よって n が4の倍数のとき，フェルマーの大定理は正しい．

もし，フェルマーの大定理が奇素数 p に対して正しいならば，上記と同様な変形により，n が p の倍数のときも正しい．3以上の自然数 n がもし奇素数で割れなければ，n は2の巾(べき)となり，よって4で割れる．つまりフェルマーの大定理は，すべての奇素数に対して正しいことが証明出来れば十分である．

$n=3$ のとき，オイラー(1770)が不完全ながら証明し，後に多くの

数学者が完全な証明にした．

$n=5$ のとき，ドイツの数学者ディリクレ(1825)が不完全な証明をしたが，同年フランスの数学者ルジャンドルが完全な別証明を与えた．

$n=7$ のとき，ラメ(1839)が証明した．

その後，クンマー(1810–1893)が現われ，虚数よりもっと広い**理想数の世界**を考え出し，多くの実りある成果をあげた．クンマーの作り出した理論をもとにして電子計算機を使い，現在では $p<125000$ ならばフェルマーの大定理が正しいことが確かめられている．

フェルマーの大定理に少し制限を加え

(7)　$$x^p+y^p=z^p,\quad p=\text{奇素数},\quad (xyz,p)=1$$

に自然数解がない，という予想をフェルマーの大定理の**第1の場合**という．つまり p と素である解は存在しないだろう，という予想である．制限があるため，その制限を利用して，一般の場合より多くの結果が得られている．たとえば，もし(7)に解があるならば

(8)　$$2^{p-1}-1 \text{ は } p^2 \text{ の倍数}$$

(9)　$$3^{p-1}-1 \text{ は } p^2 \text{ の倍数}$$

でなければならない，という結果がある．(8)が成り立つ素数 p は $p<3\times10^9$ の範囲に1093と3511の2つしかない．また(9)が成り立つ素数 p は $p<10^7$ の範囲に11と1006003の2つしかない．よって $p<3\times10^9$ の範囲では第1の場合は正しいわけである．その他の結果を使うと $p<57\times10^9$ ならば，第1の場合は正しいことが確かめられている．

§7　階乗について

大きな数を作り出すために，或る数の**階乗**を作ることはよく行われる．まず階乗の意味からはじめよう．たとえば

$$4 \times 3 \times 2 \times 1 = 24$$
$$5 \times 4 \times 3 \times 2 \times 1 = 120$$

などをそれぞれ4!, 5! と書き，4の階乗，5の階乗と呼ぶ．一般に n の階乗とは

$$n! = n \times (n-1) \times (n-2) \times \cdots \times 3 \times 2 \times 1$$

という数を表わすわけである．100の階乗は

$$100! = 100 \times 99 \times 98 \times 97 \times \cdots \times 3 \times 2 \times 1$$
$$\fallingdotseq 9.3326 \times 10^{157}$$

となることが知られている．つまり158桁の数である．あまりにも大きな数になるので驚いて！という記号を使うようになったという人もいる．

100! を素因子分解するにはどうしたらよいだろうか．この158桁の数ははじめから100個の因子に分解されているので，それらの因子をさらに素因子に分解すればよい．すなわち

$$100! = 100 \times 99 \times 98 \times 97 \times \cdots \times 3 \times 2 \times 1$$
$$= (2^2 \cdot 5^2) \times (3^2 \cdot 11) \times (2 \cdot 7^2) \times 97 \times \cdots \times 3 \times 2 \times 1$$

と直してから2の巾，3の巾，…, 97の巾をまとめればよい．例として，3の指数を上手に数えてみよう．

まず素因子に3を含むものは，3の倍数である．3の倍数は

$$3,\ 6,\ 9,\ \cdots,\ 99$$

と全部で33個ある．3つおきにあるので $[100/3]=33$ と計算出来る．前にも書いたが [　] はガウス記号，つまり実数 α に対して $[\alpha]$ は α の整数部を表わす．33個の中に 3^2 で割れるものがある．それらは9の倍数で

$$9,\ 18,\ \cdots,\ 99$$

と11個ある．3の倍数の中で3つおきにあるから $[33/3]=11$ と個数が計算される．この中で 3^3 で割れるもの，つまり27の倍数は

$$27,\ 54,\ 81$$

の3個である．9の倍数の中で3つおきにあるので $[11/3]=3$ として個数が計算出来る．さらに 3^4 で割れるものは，3番目の

$$81$$

の1個である．よって $100!$ における3の指数は

$$33+11+3+1=48$$

となる．なぜならば，たとえば $54=2\cdot3^3$ であるが，54は3の倍数，3^2 の倍数，3^3 の倍数として3重に数えられるから，これで54における3の指数が正確に数えられるわけである．同様に2の指数は

$$[100/2]=50=2 \text{ の倍数の個数}$$
$$[50/2]=25=2^2 \text{ の倍数の個数}$$
$$[25/2]=12=2^3 \text{ の倍数の個数}$$
$$[12/2]=6=2^4 \text{ の倍数の個数}$$
$$[6/2]=3=2^5 \text{ の倍数の個数}$$
$$[3/2]=1=2^6 \text{ の倍数の個数}$$

から

$$50+25+12+6+3+1=97$$

となる．他の指数も同様に計算すると

$$100!=2^{97}\cdot3^{48}\cdot5^{24}\cdot7^{16}\cdot11^{9}\cdot13^{7}\cdot17^{5}\cdot19^{5}\cdot23^{4}\cdot$$
$$29^{3}\cdot31^{3}\cdot37^{2}\cdot41^{2}\cdot43^{2}\cdot47^{2}\cdot53\cdot59\cdot61\cdot$$
$$67\cdot71\cdot73\cdot79\cdot83\cdot89\cdot97$$

となる．

一般に $n!$ を素因子分解すると，素数 p の指数 e_p は

(1)
$$e_p=[n/p]+[n/p^2]+[n/p^3]+\cdots$$
$$=\sum_{m=1}^{\infty}[n/p^m]$$

となる．$p^k\leqq n<p^{k+1}$ と k を定めれば $k+1\leqq m$ のとき $[n/p^m]=0$ で

あるから，(1)の右辺の和は実質的には有限個の和

$$e_p = [n/p]+[n/p^2]+[n/p^3]+\cdots+[n/p^k]$$

を意味する．さて(1)の証明をする．1からnまでの数の中でpの倍数は$n=p\cdot q+r$ $(0\leqq r<p)$としたとき

$$p,\ 2p,\ 3p,\ \cdots,\ qp$$

のq個である．

$$n/p = q+r/p, \qquad 0\leqq r/p<1$$

であるから$q=[n/p]$と表わせる．p^2で割れるものは，同様に考えると$[n/p^2]$個ある．$p^3, p^4, \cdots$で割れるものは$[n/p^3]$個，$[n/p^4]$個，…ある．これらの中で，たとえばp^3で割れてp^4で割れない数はpの指数に3だけ影響を与えるが，pの倍数，p^2の倍数，p^3の倍数として3重に数えられればちょうどよい．よって(1)が示された．

例　αを実数，mを自然数とするとき，次の式を示せ．

(2)
$$[\alpha+m] = [\alpha]+m$$

(3)
$$\left[\frac{\alpha}{m}\right] = \left[\frac{[\alpha]}{m}\right].$$

解　(2)の証明　$[\alpha]=t$とすると$\alpha=t+\beta, 0\leqq\beta<1$となる．$\alpha+m=(t+m)+\beta$であるから

$$[\alpha+m] = t+m = [\alpha]+m.$$

(3)の証明　$[\alpha/m]=q$とおけば

$$\alpha/m\geqq q, \qquad \therefore\quad \alpha\geqq mq$$

となる．mqは整数であるから$[\alpha]\geqq mq$となり

$$\alpha/m\geqq[\alpha]/m\geqq mq/m=q$$

となる．よってガウス記号の意味を考えれば

$$q=[\alpha/m]\geqq[[\alpha]/m]\geqq q$$

となり(3)が得られた．——

例　上記の例で，$\alpha=n/p^e, m=p$とおくと

$$\left[\frac{n}{p^{e+1}}\right]=\left[\frac{[n/p^e]}{p}\right]$$

となる．よって左辺を計算するとき，あらかじめ$[n/p^e]$が計算されていれば，その値をpで割ればよい．よってe_pを計算するとき，$[n/p], [n/p^2], \cdots$という列は順に前の値をpで割り，その整数部を求めればよい．——

例　$\dfrac{(m+n)!}{m!n!}$は整数であることを示せ．

解　αとβを実数とし，整数部と小数部に分けて

$$\alpha=[\alpha]+\gamma, \qquad 0\leqq\gamma<1$$
$$\beta=[\beta]+\delta, \qquad 0\leqq\delta<1$$

とすれば

$$\alpha+\beta=[\alpha]+[\beta]+(\gamma+\delta), \qquad 0\leqq\gamma+\delta<2$$

となる．よって

$$\begin{aligned}[\alpha+\beta]&=[\alpha]+[\beta], & \gamma+\delta<1 \text{ のとき}\\ &=[\alpha]+[\beta]+1, & \gamma+\delta\geqq 1 \text{ のとき}\end{aligned}$$

となり

$$[\alpha+\beta]\geqq[\alpha]+[\beta]$$

が得られる．$\alpha=m/p^e, \beta=n/p^e$とおくと

$$[(m+n)/p^e]\geqq[m/p^e]+[n/p^e]$$

となる．$e=1, 2, 3, \cdots$とおき，加えると

$$\sum_{e=1}^{\infty}\left[\frac{m+n}{p^e}\right]\geqq\sum_{e=1}^{\infty}\left[\frac{m}{p^e}\right]+\sum_{e=1}^{\infty}\left[\frac{n}{p^e}\right]$$

となる．左辺は$(m+n)!$のpの指数であり，右辺は$m!\cdot n!$のpの指数であるから，問題の式のpの指数は分子の方が分母より大きいか，等しい．すべての素数に対してこのことが言えるので，問題の式は整数である．——

次に $n!$ のだいたいの大きさを評価するために，自然対数をとると

$$\log n! = \log 2+\log 3+\cdots+\log n$$

となる．もし右辺の値がわかれば，その値を a とすれば，$n!=e^a$ と計算することが出来る．a のだいたいの大きさを求めるために，対数関数 $y=\log_e x$ のグラフを考えてみよう(図 4-1)．

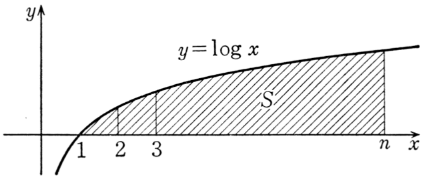


図 4-1

積分の定義から

$$\int_1^n \log x dx = S \text{ の面積}$$

である．対数関数は増加関数であるから，図 4-2 の面積を考えれば，

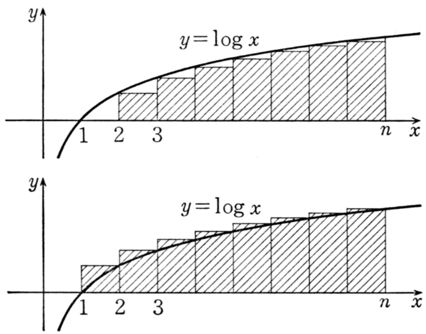


図 4-2

$$\log 2+\log 3+\cdots+\log(n-1) < \int_1^n \log x dx$$
$$< \log 2+\log 3+\cdots+\log n$$

となる．$\log n! = \log 2+\log 3+\cdots+\log n$ であるから

$$\int_1^n \log x dx < \log n! < \int_1^n \log x dx + \log n$$

となる．部分積分から

$$\int_1^n \log x dx = [x \log x]_1^n - \int_1^n x \cdot \frac{1}{x} dx$$
$$= [x \log x]_1^n - [x]_1^n$$
$$= n \log n - n + 1$$

となり

(4)　　$n \log n - n + 1 < \log n! < (n+1)\log n - n + 1$

が得られた．よってこの式の左辺を b，右辺を c とすれば $e^b < n! < e^c$ が得られる．

例　$n=100$ のときを考えると，常用対数は

$$\log_{10}(100!) = \log_e(100!)/\log_e 10$$

であるから

$$(100 \log 100 - 100 + 1)/\log 10 \doteqdot 157.0048$$
$$(101 \log 100 - 100 + 1)/\log 10 \doteqdot 159.0048$$

から $157 < \log_{10} n! < 160$ となり

$$10^{157} < n! < 10^{160}$$

が得られる．——

§8　$n<p<n^2$ となる素数の存在

一般に 2 以上の自然数 n に対して $n<p<2n$ となる素数が存在するが，その証明は大変なので，ここでは $n<p<n^2$ となる素数が存在

することを示そう(内山三郎教授による証明).

まず$(n^2)!$ および$(n!)^n$ を割るpの指数は前節の(1)から

$$\sum_{m=1}^{\infty}\left[\frac{n^2}{p^m}\right] \quad \text{および} \quad n\sum_{m=1}^{\infty}\left[\frac{n}{p^m}\right]$$

であるから$(n^2)!/(n!)^n$ のpの指数a_pは

$$\begin{aligned} a_p &= \sum_{m=1}^{\infty}[n^2/p^m]-n\sum_{m=1}^{\infty}[n/p^m] \\ &= \sum_{m=1}^{\infty}[n^2/p^m]-\sum_{m=1}^{\infty}n[n/p^m] \\ &= \sum_{m=1}^{\infty}\left(\left[\frac{n^2}{p^m}\right]-n\left[\frac{n}{p^m}\right]\right) \end{aligned}$$

となる. よって

(1) $$\frac{(n^2)!}{(n!)^n} = \prod_{p<n^2} p^{a_p}$$

となる. 右辺の積は$p<n^2$ となるすべての素数pに対しての積になる. $p>n^2$ ならば, $a_p=0$ となるので, (1)は成り立つ.

$2\leqq n\leqq 14$ のときは

$$2 < 3 < 2^2$$
$$3, 4 < 5 < 3^2, 4^2$$
$$5, 6, \cdots, 14 < 17 < 5^2, 6^2, \cdots, 14^2$$

であるから$n<p<n^2$ となる素数は存在する. よって$n\geqq 15$ のときを証明すればよい. 背理法を用い, 或るnに対して$n<p<n^2$ となる素数が1つもないと仮定する. このときn^2 より小さな素数はn以下であるから(1)から

$$\frac{(n^2)!}{(n!)^n} = \prod_{p<n^2} p^{a_p} = \prod_{p\leqq n} p^{a_p}$$

となる. n/p^m を整数部と小数部に分け

$$n/p^m = q+\alpha, \qquad q = [n/p^m], \qquad 0 \leqq \alpha < 1$$

とすれば

$$n[n/p^m] = nq$$

となり，$n^2/p^m = n\cdot(n/p^m)$ から

$$\begin{aligned}[n^2/p^m] &= [nq+n\alpha] \\ &= nq+[n\alpha]\end{aligned}$$

となる．$0 \leqq n\alpha < n$ であるから

$$0 \leqq [n\alpha] < n$$

となる．よって

$$\left[\frac{n^2}{p^m}\right] - n\left[\frac{n}{p^m}\right] = nq+[n\alpha]-nq < n$$

となるから，r を $p^r \leqq n^2 < p^{r+1}$ になるように定めれば，$r<m$ のとき $0<n^2/p^m<1, 0<n/p^m<1$ となり，$[n^2/p^m]=0, [n/p^m]=0$ となる．よって

$$\begin{aligned}a_p &= \sum_{m=1}^{\infty}\left(\left[\frac{n^2}{p^m}\right]-n\left[\frac{n}{p^m}\right]\right) \\ &= \sum_{m=1}^{r}\left(\left[\frac{n^2}{p^m}\right]-n\left[\frac{n}{p^m}\right]\right) \\ &< rn.\end{aligned}$$

$\pi(n)$ を n 以下の素数の個数とすれば，$p^r \leqq n^2$ から

$$\prod_{p\leqq n} p^{a_p} < \prod_{p \leqq n} p^{rn} \leqq \prod_{p\leqq n} n^{2n} = n^{2n\cdot\pi(n)}$$

が得られた．よって

$$(n^2)!/(n!)^n < n^{2n\cdot\pi(n)}$$

となる．この両辺の対数をとり，前節の(4)を用いると，

$$\begin{aligned}2n\cdot\pi(n)\cdot\log n &> \log((n^2)!)-n\log(n!) \\ &> (n^2\log n^2-n^2+1)-n(n\log n-n+1+\log n) \\ &= n^2\log n+1-n-n\log n \\ &> n^2\log n-n-n\log n\end{aligned}$$

となり，$n \geqq 15$ から $\log n > 1$ であるから

$$2n \cdot \pi(n) \cdot \log n > n^2 \log n - 2n \log n$$

となる．両辺を $2n \log n$ で割れば

(2) $$\pi(n) > n/2 - 1 = (n-2)/2$$

となる．ところが事実は逆である．n 以下の奇数は

$$n = \text{偶数ならば} \quad n/2 \text{ 個}$$

$$n = \text{奇数ならば} \quad (n+1)/2 \text{ 個}$$

しかなく，$n(\geqq 15)$ 以下の素数は 2 または 1, 9, 15 以外の奇数である．よって

(3) $$\pi(n) \leqq 1 + (n+1)/2 - 3 = (n-3)/2$$

となる．(2) と (3) は矛盾している．$n < p < n^2$ となる素数が存在しないと仮定したので，矛盾が生じた．よって $n < p < n^2$ となる素数は必ず存在する．

第5章 合 同 式

§1 合同式の定義と意味

a, b を整数，m を自然数とする．もし $a-b$ が m で割れるとき a と b は m を**法**として**合同**である，といい，記号で

$$a \equiv b \pmod{m}$$

と書く．また $a-b$ が m で割り切れないとき

$$a \not\equiv b \pmod{m}$$

と書き a と b は $\mathrm{mod}\, m$ で**不合同**という．

例 $104-53 = 51 = 17\times 3$

$$\therefore \quad 104 \equiv 53 \pmod{17}. \text{ ——}$$

a, b を m で割り

$$a = mq_1+r_1 \qquad (0 \leqq r_1 < m)$$

$$b = mq_2+r_2 \qquad (0 \leqq r_2 < m)$$

のとき

$$a-b = m(q_1-q_2)+(r_1-r_2) \qquad (-m < r_1-r_2 < m)$$

となるので，$a-b$ が m で割れることと，r_1-r_2 が m で割れることは同じである．r_1-r_2 が m で割れることは $r_1=r_2$ を意味する．よって a と b が m を法として合同である，とは a, b を m で割ったときの余りが等しいことを意味する．つまり m の倍数の差を無視した余りを考えれば等しいということである．このように $\equiv$ で結ばれた式のことを**合同式**という．

例

$$104 = 17\cdot 6+2$$

$$53 = 17\cdot 3+2$$

$$\therefore \quad 104 \equiv 53 \pmod{17}. \text{ ——}$$

合同式の基本的な性質は

(1)　　$a \equiv a \pmod{m}$

(2)　　$a \equiv b \pmod{m}$　ならば　$b \equiv a \pmod{m}$

(3)　　$a \equiv b \pmod{m}$,　　$b \equiv c \pmod{m}$

ならば　$a \equiv c \pmod{m}$

である．(1)は $a-a=0$ が m の倍数であることから得られる．(2)は $a-b$ が m で割れれば $b-a=-(a-b)$ も m で割れることから得られる．(3)は $a-b$ が m で割れ，$b-c$ が m で割れれば

$$a-c = (a-b)+(b-c)$$

も m で割れることから得られる．(1), (2), (3) とも等式と似た性質である．

そもそも等式とは何か，自然数とは何か，と考えてみよう．この世の中には完全に同じものはない．しかし2つの物体AとBとは大きさが等しい，重さが等しい，などという．AとBは別物ではあるが，大きさとか重さとか，何か共通の性質を持っているとき，その性質について等しいとか等しくない，という言葉を使う．自然数についても同じことが言える．たとえば三という物体はない．三という言葉は3本の鉛筆，3個のリンゴ，3冊の本，…等に共通した性質として，性質を表わす言葉として生まれてきた．よって三という名を持つ物体はなく，三は自然界の或る性質を抽象化して生まれた言葉である．抽象化とは組分けをすることである．同じ性質を持つものを1組にまとめ，その組に名前を付けることである．

おおげさな表現をすれば，合同式は整数全体をいまひとたび抽象化することである．m で割ったとき，余りが等しいものを1つの組にして組分けすることである．m を法として組分けをすると，m 個の組が出来る．同じ組に入っている2つの数は合同である．たとえば $m=2$ の場合を考えよう．2で割ったとき，余りが0か1かによ

り整数全体は2組に分れる．そのうち余りが0となる組に対して偶数という名前を付け，1余る組に対しては奇数という名前を付けるわけである．すべての日付を7日目ごとに分類すると，7組に分れ，それらの組に日曜日，月曜日，…，土曜日という名前が付けられている．つまり曜日とはすべての日付を mod 7 で分類したものである．

組のことを**類**といい，組分けすることを**類別する**ともいう．

以上のように合同式は，深い意味を持つけれど，定義そのものは非常に素朴である．ガウスは整数をもう一度抽象化したものだという意味を含め，合同式を $a \equiv b$ と表わす記号を思い付いた．この記号のおかげで，整数論はとても見通しがよくなった．

§2　合同式の四則

2つの合同式

$$a \equiv b \pmod m$$
$$c \equiv d \pmod m$$

があったとき，定義から $a-b, c-d$ は m の倍数である．よって

$$(a+c)-(b+d) = (a-b)+(c-d)$$
$$(a-c)-(b-d) = (a-b)-(c-d)$$

も m の倍数である．また

$$\begin{aligned} ac-bd &= ac-ad+ad-bd \\ &= a(c-d)+(a-b)d \end{aligned}$$

も m の倍数である．よって次の定理が得られた．

定理 7　2つの合同式

$$a \equiv b \pmod m$$
$$c \equiv d \pmod m$$

があったとき，足しても，引いても，掛けても合同である．つまり

$$a+c \equiv b+d \pmod m$$

$$a-c \equiv b-d \pmod{m}$$
$$a\times c \equiv b\times d \pmod{m}$$

が成り立つ．——

この定理を2回使えば

$$a \equiv b \pmod{m}$$
$$c \equiv d \pmod{m}$$
$$e \equiv f \pmod{m}$$

のはじめの2式から

$$a+c \equiv b+d \pmod{m}$$

が得られ，この式と3番目の式から

$$(a+c)+e \equiv (b+d)+f \pmod{m}$$

が得られる．同様にして3つ以上の合同式を掛けても合同である．

また $c\equiv c \pmod{m}$ であるから

$$ac \equiv bc \pmod{m}$$

も得られる．つまり両辺に同じ数を掛けてもよい．

例
$$10 \equiv 1 \pmod{9}$$
$$10 \equiv 1 \pmod{9}$$

と同じ式を2つ作り，辺々掛けると

$$10^2 \equiv 1 \pmod{9}$$

が得られる．この式にはじめの式を掛ければ

$$10^3 \equiv 1 \pmod{9}$$

が得られる．同様につづけると

$$10^n \equiv 1 \pmod{9}$$

が得られる．——

例　$10^5\equiv 1 \pmod{9}$ の両辺に6を掛けて

$$6\times 10^5 \equiv 6 \pmod{9}$$

が得られる．同様にして次の変形が得られる．

$$\begin{aligned}654321 &= 6\times10^5+5\times10^4+4\times10^3+3\times10^2+2\times10+1\\ &\equiv 6\times1+5\times1+4\times1+3\times1+2\times1+1 \pmod 9\\ &= 21\\ &= 2\times10+1\\ &\equiv 2\times1+1 \pmod 9\\ &= 3.\end{aligned}$$

よって 654321 を 9 で割ると余りは 3 となる．――

例　$10\equiv1 \pmod 3$ を利用すれば，3 で割った余りは各桁を加えて得られる．――

例

$$10 \equiv -1 \pmod{11}$$

であるから，この式を何回も掛け合せ

$$10^n \equiv (-1)^n \pmod{11}$$

が得られる．よって

$$\begin{aligned}123456 &= 1\times10^5+2\times10^4+3\times10^3+4\times10^2+5\times10+6\\ &\equiv -1+2-3+4-5+6 \pmod{11}\\ &= 3\end{aligned}$$

つまり 123456 を 11 で割れば余りが 3 となる．――

例　$1001=7\times11\times13$ であるから

$$1000 \equiv -1 \pmod 7$$

$$(1000)^n \equiv (-1)^n \pmod 7$$

となる．よって 987654321 を 7 で割った余りは

$$\begin{aligned}987654321 &= 987\times(1000)^2+654\times1000+321\\ &\equiv 987-654+321 \pmod 7\\ &= 654\end{aligned}$$

から 654 を 7 で割った余りに等しい．つまり 3 が余りとなる．同様に 987654321 を 13 で割った余りは 654 を 13 で割った余りに等しい．つまり 4 となる．――

例　6桁の数789012は7で割り切れる:

$$\begin{aligned} 789012 &\equiv -789+012 \pmod 7 \\ &= -777. \end{aligned}$$

このとき，最下位の数を最上位に順に持っていった278901等も7で割り切れる:

$$\begin{aligned} 789012 &= 7\times 112716 \\ 278901 &= 7\times 39843 \\ 127890 &= 7\times 18270 \\ 012789 &= 7\times 1827 \\ 901278 &= 7\times 128754 \\ 890127 &= 7\times 127161. \end{aligned}$$

一般に6桁の数が7で割り切れるならば，その数の最下位の数を最上位に持っていって出来た数も7で割れる．その理由は，6桁の数を上5桁xと下1桁yに分けて$10x+y$と表わせば，最下位を最上位に持っていった数は$y\times 10^5+x$となる．この数が7で割れることを言えばよい．

$$\begin{aligned} (y\times 10^5+x)\times 10 &= y\cdot(1000)^2+10x \\ &\equiv y+10x \pmod 7 \end{aligned}$$

となり，仮定から$10x+y$は7で割れる．よって左辺も7で割れる．$(10, 7)=1$であるから$y\times 10^5+x$が7で割れることが得られた．——

定理7の本質的な意味は次のようになる:

整数全体を$\bmod m$で分類するとm個の類(組)が出来る．つまりmで割ったとき割り切れるものを1まとめにし，1余るもの，2余るもの，…，$m-1$余るものをそれぞれ1まとめにするわけである．このように類別したとき，1つの類Aから1つの数aを選び，類Cから1つの数cを選んだとき，$a+c, a-c, a\cdot c$の属する類はaやcの選び方に無関係に定まる．よってそれらを$A+C, A-C, A\times C$と

書いてもさしつかえないであろう．このように類同士に加法，減法，乗法が出来る．これが一段と高い場所からながめた定理7の姿である．

§3　1次合同式

等式においては，両辺を0でない数で割ることが出来る．合同式においては，0でないという条件は“mと互いに素である”という条件となる．

$$ac \equiv bc \pmod m, \qquad (c, m) = 1$$

のとき，$ac-bc=(a-b)\cdot c$はmで割れる．$(c, m)=1$から定理3を使えば$a-b$がmで割れることが導かれる．つまり$a\equiv b \pmod m$となり，合同式においては両辺をmと互いに素な数で割ってもよいことが得られた．

次に1次合同式

$$ax \equiv b \pmod m \tag{1}$$

を考えよう．等式ならば，両辺をaで割りxが得られる．ただし$a\neq 0$でなければならない．合同式においても，$(a, m)=1$ならば(1)は必ず解を持つ．何故ならば定理2から

$$ax_1+my_1 = 1$$

となる整数x_1, y_1が存在する．よって

$$ax_1 \equiv 1 \pmod m$$

が得られる．両辺をb倍すれば

$$a(bx_1) \equiv b \pmod m$$

であるから$x=bx_1$が1つの解となる．他に解x'があったとして

$$ax' \equiv b \pmod m$$

とする．(1)からこの式を引くと

$$a(x-x') \equiv 0 \pmod m$$

となる．よって $a(x-x')$ が m で割れるけれど，$(a, m)=1$ から $x-x'$ が m で割れる．つまり他に解があったとすると

$$x \equiv x' \pmod{m} \tag{2}$$

でなければならない．逆に(2)が成り立てば

$$ax \equiv ax' \pmod{m}$$

であるから x' は(1)の解となる．まとめると次のようになる．

定理8　$(a, m)=1$ のとき1次合同式

$$ax \equiv b \pmod{m}$$

の解は存在する．解は m を法としてただ1つである．——

整数全体を mod m で分類すれば，m 個の類に分れる．そのうちの或る類に属する数はすべて解であり，他の類に属する数はどれも解にならない，という意味である．

例　$7x\equiv 2 \pmod{22}$ を解け．

解

$$22 = 7\cdot 3+1$$
$$7 = 1\cdot 7+0$$

であるから $(7, 22)=1$ となり解は mod 22 でただ1つ定まる．

$$22-7\cdot 3 = 1$$

であるから

$$7(-3) \equiv 1 \pmod{22}$$

となり，2倍すれば

$$7(-6) \equiv 2 \pmod{22}$$

となる．よって解は

$$x \equiv -6 \pmod{22}$$

となる．——

$(a, m)=d>1$ の場合，(1)の解はどうなるだろうか．もし(1)が解 x を持てば $ax-b$ が m で割れるので

$$ax-b = my$$

となる整数 y が存在する．$a=a_1\cdot d$, $m=m_1\cdot d$ とおけば $(a_1, m_1)=1$ となり，

$$
\begin{aligned}
b &= ax-my \\
&= (a_1x-m_1y)d
\end{aligned}
$$

であるから b は d の倍数でなければならない．

逆に b が d で割れ，$b=b_1\cdot d$ となるとき，$(a_1, m_1)=1$ であるから，定理 8 から

$$a_1x \equiv b_1 \pmod{m_1}$$

となる解が存在する，つまり a_1x-b_1 は m_1 で割れる．よって $(a_1x-b_1)d$ は m_1d で割れる．書き直すと $ax-b$ は m で割れる．つまり

$$ax \equiv b \pmod{m}$$

となる．他に解 x' があったとすると，$a(x-x')$ が m で割れる．よって $a_1(x-x')$ が m_1 で割れる．$(a_1, m_1)=1$ から $x-x'$ が m_1 で割れる．逆に $x-x'$ が m_1 で割れれば $a_1(x-x')$ が m_1 で割れ，d 倍して $a(x-x')$ が m で割れ

$$
\begin{aligned}
ax' &\equiv ax \pmod{m} \\
&\equiv b \pmod{m}
\end{aligned}
$$

となり解となる．まとめると，次の定理となる．

定理 9 $(a, m)=d, m=m_1d$ のとき

$$ax \equiv b \pmod{m}$$

の解が存在するための必要十分条件は，b が d の倍数となることである．b が d の倍数のとき，1つの解を x とすればすべての解は $\mathrm{mod}\, m$ で考えると

$$x,\ x+m_1,\ x+2x_1,\ \cdots,\ x+(d-1)m_1$$

を含む，d 個の類である．——

つまり $\mathrm{mod}\, m$ で考えると d 個の解があるわけである．$d=1$ の場合が定理 8 である．$\mathrm{mod}\, m_1$ で考えれば解は 1 つである．

具体的に合同式を解くには互除法を用いればよいけれども，実質的には同じであるが，次の方法が見通しがよい．

$$ax \equiv b \pmod{m}$$

を解くために x が何であっても成り立つ自明な式

$$mx \equiv 0 \pmod{m}$$

を利用する．x の係数を互除法で小さくしてゆくと解が得られる．

例

$$7x \equiv 2 \pmod{22}$$

を解くには自明な式

$$22x \equiv 0 \pmod{22}$$

を利用する．$22=7\times3+1$ であるから $7x\equiv2$ を3倍して

$$21x \equiv 6 \pmod{22}$$

を得る．$22x\equiv0$ から引くと

$$x \equiv -6 \pmod{22}$$

が得られる．——

例　$4676x\equiv7 \pmod{1141}$ を解け．

解　自明な式

(3)
$$1141x \equiv 0 \pmod{1141}$$

を利用する．$4676=1141\times4+112$ であるから，(3)の両辺を4倍し，与式から引くと

(4)
$$112x \equiv 7 \pmod{1141}$$

となる．$1141=112\times10+21$ であるから，(4)の両辺を10倍して(3)から引くと

(5)
$$21x \equiv -70 \pmod{1141}$$

が得られる．$112=21\times5+7$ であるから(5)を5倍して(4)から引くと

(6)
$$7x \equiv 357 \pmod{1141}$$

となる．$21=7\times3$ であるから $(4676, 1141)=7$ であることがわかっ

た．与式の右辺は確かに 7 で割れるから，与式は解を持つ．(6) から $7x-357$ が 1141 で割れる．$357=7\times51$, $1141=7\times163$ であるから 7 で割り $x-51$ が 163 で割れる．よって

$$x \equiv 51 \pmod{163}$$

が解である．mod 1141 で考えれば

$$x \equiv 51, 214, 377, 540, 703, 866, 1029 \pmod{1141}$$

の 7 個の類が解となる．——

このように

$$ax \equiv b \pmod{m}$$
$$mx \equiv 0 \pmod{m}$$

と 2 つ式をならべ，x の係数を互除法で小さくしてゆくと，右辺に自動的に解が得られるわけである．

例　不定方程式 $17x+13y=5$ を解け．

解　mod 13 で考えれば

(7) $$17x \equiv 5 \pmod{13}$$

となる．自明な式

(8) $$13x \equiv 0 \pmod{13}$$

を利用し，(7) から引けば

(9) $$4x \equiv 5 \pmod{13}$$

となる．$13=4\times3+1$ であるから (9) を 3 倍し，(8) から引けば

(10) $$\begin{aligned} x &\equiv -15 \pmod{13} \\ &\equiv -2 \pmod{13} \end{aligned}$$

となる．つまり $x=-2+13t$ が解となる．この式を与式に代入すると

$$\begin{aligned} 13y &= 5-17x \\ &= 5-17(-2+13t) \\ &= 5+34-17\times13t \end{aligned}$$

$$= 13\times 3-17\times 13t$$

つまり $y=3-17t$ となり

$$\begin{cases} x = -2+13t \\ y = 3-17t \qquad (t\text{は整数}) \end{cases}$$

が一般解となる．——

このように不定方程式も合同式に直すと変数が1つ少なくなり，見通しよく解ける．

例 7で割れば3余り，11で割れば5余り，13で割れば6余る数を求めよ．

解 求める数を x とすれば

(11) $$x \equiv 3 \pmod 7$$

(12) $$x \equiv 5 \pmod{11}$$

(13) $$x \equiv 6 \pmod{13}$$

となる．(11)から $x=7y+3$ となる整数 y が存在する．この式を(12)に代入すると

$$7y+3 \equiv 5 \pmod{11}$$

(14) $$7y \equiv 2 \pmod{11}$$

となる．自明な式

(15) $$11y \equiv 0 \pmod{11}$$

から(14)を引くと

(16) $$4y \equiv -2 \pmod{11}$$

となる．(16)の両辺を2倍して(14)を引くと

$$y \equiv -6 \pmod{11}$$
$$\equiv 5 \pmod{11}$$

となる．よって $y=11z+5$ となる整数 z が存在する．この式を(13)に代入すると

$$6 \equiv x \pmod{13}$$

$$
\begin{aligned}
&= 7y+3\\
&= 7(11z+5)+3\\
&= 77z+38\\
&\equiv -z+12 \pmod{13}
\end{aligned}
$$

となり $z\equiv 6 \pmod{13}$，つまり $z=13t+6$ となる．よって

$$
\begin{aligned}
x &= 77z+38\\
&= 77(13t+6)+38\\
&= 1001t+500
\end{aligned}
$$

となる．——

類同士に加法，減法，乗法が行なえる，という立場からみれば，1 次合同式は類 A, B に対して

$$AX = B$$

となる類 X を求めることである．一段と高い立場から見ると，合同式は等式なのである．$a\equiv a' \pmod{m}$ ならば $a=m\cdot q+a'$ と書ける．このとき，互除法の証明(定理 1)からわかるように $(a, m)=(a', m)$ となる．よって a と m が互いに素である，という性質は，a を同じ類の中の数でおきかえても成り立つ．つまり，a の属する類 A の性質である．$(a, m)=1$ のとき，a の属する類を**既約類**という．定理 8 は A が既約類ならば，$AX=B$ はただ 1 つの解を持つ，という内容である．

§4　n 次合同式

法 m に対して $a_0\not\equiv 0 \pmod{m}$ のとき

$$f(x) = a_0x^n+a_1x^{n-1}+\cdots+a_n \equiv 0 \pmod{m}$$

を **n 次合同式**という．1 次合同式の場合と異なり，解があるか否か，あるときは能率よく求めるにはどうしたらよいか，などの一般論はない．しかし解の個数については次のようなことが言える．

$$x \equiv x_1 \pmod{m} \quad ならば \quad x^k \equiv {x_1}^k.$$

よって $a_{n-k}x^k \equiv a_{n-k}{x_1}^k$ となり，$f(x) \equiv f(x_1)$ が得られる．よって解の個数として mod m で分類したときの解を含む類の個数が有限の値として定まる．

さて $m=p=$素数 の場合を考えよう．このとき $a_0 \not\equiv 0 \pmod{p}$ は $(a_0, p)=1$ を意味する．$n=1$ のときは，解は mod p で考えるとただ1つある．$n \geqq 2$ のときは，解は mod p で考えると，多くとも n 個以下であることが証明出来る．

例　$x^2+1 \equiv 0 \pmod{5}$ を解け．

解　$x \equiv x_1 \pmod{5}$ ならば $x^2 \equiv {x_1}^2$ であるから $x^2+1 \equiv {x_1}^2+1$ となる．よって $x=0, 1, \cdots, 4$ の場合に調べればよい．

$$0^2+1=1, \quad 1^2+1=2, \quad 2^2+1=5\equiv 0,$$
$$3^2+1=10\equiv 0, \quad 4^2+1=17\equiv 2.$$

よって2および3を含む2つの類が解である．——

例　$x^2+1 \equiv 0 \pmod{7}$ を解け．

解　$x=0, 1, 2, \cdots, 6$ を代入すると

$$0^2+1=1, \quad 1^2+1=2, \quad 2^2+1=5, \quad 3^2+1=10\equiv 3,$$
$$4^2+1=17\equiv 3, \quad 5^2+1=26\equiv 5, \quad 6^2+1=37\equiv 2$$

となり解が1つもない．——

さて解が n 個以下であることを帰納法で示そう．

$n=1$ のときは定理8から正しい．$n-1$ 次以下の場合を正しいと仮定する．$f(x)$ が n 次式のとき，解が1つもないこともある．1つもないことは，解が0個であるからこれ以上言うことはない．よって b という解を持ったとする．つまり $f(b) \equiv 0 \pmod{p}$ となったとする．このとき多項式 $f(x)$ を普通の意味で $x-b$ で割ると，余りは定数となり

$$(1) \qquad f(x) = (x-b)\cdot g(x) + r \qquad (r\text{ は定数})$$

となる．この(1)に $x=b$ を代入すると

$$f(b) = 0\cdot g(x)+r$$
$$= r$$

となり $f(b)\equiv 0 \pmod p$ から $r\equiv 0 \pmod p$ となる．$f(x)\equiv 0 \pmod p$ に他の解 c があったとすると，(1)から

$$f(c) = (c-b)\cdot g(c)+r$$
$$\equiv (c-b)\cdot g(c) \pmod p$$

となる．$f(c)\equiv 0$ から $(c-b)\cdot g(c)$ は素数 p で割れる．よって $c-b$ または $g(c)$ が素数 p で割れる．これは $c\equiv b \pmod p$ または $g(c)\equiv 0 \pmod p$ を意味する．$c\equiv b \pmod p$ のときは，c と b は同じ類に入るから $\mathrm{mod}\, p$ で考えたときは解としては同一である．よって，この場合以外を考えると $g(c)\equiv 0 \pmod p$ でなければならない．$g(x)$ は $n-1$ 次式であり，最高次の係数は a_0 で $(a_0, p)=1$ であるから帰納法の仮定が使えて，$g(x)\equiv 0 \pmod p$ となる解は $\mathrm{mod}\, p$ で数えると多くて $n-1$ 個である．$f(x)\equiv 0$ の解は b と $g(x)\equiv 0$ の解以外にないから，合わせて多くとも n 個しかない．まとめると次のようになる．

定理 10　p が素数，$(a_0, p)=1$ のとき，

$$f(x) = a_0x^n+a_1x^{n-1}+\cdots+a_n \equiv 0 \pmod p$$

の解は $\mathrm{mod}\, p$ で数えると，多くて n 個である．——

§5　ウィルソンの定理

自然数 p を 2 以外の素数とし，$1\leqq x\leqq p-1$ としよう．そのとき $(x, p)=1$ となるので 1 次合同式

(1)　$$xy \equiv 1 \pmod p$$

は定理 8 から $\mathrm{mod}\, p$ で考えるとただ 1 つの解を持つ．(1)から y は当然 p で割れないから，$1\leqq y\leqq p-1$ に制限すると，ただ 1 つに定まる．この y を x の配偶と呼ぼう．ときには配偶が自分自身にな

るような数もある．それを中性な数と呼ぼう．それは

$$x^2 \equiv 1 \pmod p$$

の解である．$x^2-1=(x-1)(x+1)$ が p で割れる場合であるから $x-1$ または $x+1$ が p で割れる．つまり中性な数は1または $p-1$ である．$p\neq 2$ であるから $1\neq p-1$ である．この2数以外は自分自身と異なる配偶を持つわけである．これを $x_1, x_2, \cdots, x_{(p-3)/2}$ およびその配偶 $y_1, y_2, \cdots, y_{(p-3)/2}$ と書こう．

$$1, p-1, x_1, x_2, \cdots, x_{(p-3)/2}, y_1, y_2, \cdots, y_{(p-3)/2}$$

は1から $p-1$ までの数の順を変えただけであるから，すべてを掛け合わせると同じになる．つまり

$$\begin{aligned}(p-1)! &= (p-1)\cdot(p-2)\cdot\cdots\cdot 3\cdot 2\cdot 1\\ &= 1\cdot(p-1)\cdot(x_1y_1)\cdot(x_2y_2)\cdot\cdots\cdot(x_{(p-3)/2}y_{(p-3)/2})\end{aligned}$$

となり，$x_iy_i\equiv 1$ であるから

$$\begin{aligned}&\equiv 1\cdot(p-1)\cdot 1\cdot 1\cdot\cdots\cdot 1 \pmod p\\ &\equiv -1 \pmod p\end{aligned}$$

となり $(p-1)!+1$ は p で割れる．$p=2$ のとき，$(p-1)!+1=1!+1=2$ であるからやはり p で割れる．つまりすべての素数 p に対して $(p-1)!+1$ は p の倍数である．

例

$$\begin{aligned}(2-1)!+1 &= 2 = 2\cdot 1\\ (3-1)!+1 &= 3 = 3\cdot 1\\ (5-1)!+1 &= 25 = 5\cdot 5\\ (7-1)!+1 &= 721 = 7\cdot 103\\ (11-1)!+1 &= 3628801 = 11\cdot 329891\\ (13-1)!+1 &= 479001601 = 13\cdot 36846277\\ (17-1)!+1 &= 20922789888001 = 17\cdot 1230752346353\\ (19-1)!+1 &= 6402373705728001\\ &= 19\cdot 336967037143579.\end{aligned}$$

——

$(p-1)!+1$ は p で割れるが，p^2 では割れないだろうか．前の例から $((p-1)!+1)/p$ を調べると，次のようになる．

例

$$((2-1)!+1)/2 = 1 = 2\cdot 0+1$$
$$((3-1)!+1)/3 = 1 = 3\cdot 0+1$$
$$((5-1)!+1)/5 = 5 = 5\cdot 1+0$$
$$((7-1)!+1)/7 = 103 = 7\cdot 14+5$$
$$((11-1)!+1)/11 = 329891 = 11\cdot 29990+1$$
$$((13-1)!+1)/13 = 36846277 = 13\cdot 2834329+0$$
$$((17-1)!+1)/17 = 1230752346353 = 17\cdot 72397196844+5$$
$$((19-1)!+1)/19 = 336967037143579 = 19\cdot 17735107218083+2.$$ ——

このように $p=5$ または $p=13$ のとき，$(p-1)!+1$ は p^2 で割り切れる．現在のところ $p<200183$ ならば $p=5$, 13, 563 の 3 つだけが $(p-1)!+1$ が p^2 で割れることが知られている．どのような場合，p^2 で割れるか，という一般的な性質は何もわかっていない．

以上のように素数 p に対しては $(p-1)!+1$ が p で割れるが，逆に 2 以上の自然数 a に対して $(a-1)!+1$ が a で割れれば a は素数である．何故ならば，もし a が合成数で $a=b\cdot c$, $1<b<a$ とすると，$b\leqq a-1$ であるから

$$\begin{aligned}(a-1)! &= (a-1)(a-2)\cdot\cdots\cdot 3\cdot 2\cdot 1\\ &= (a-1)\cdot\cdots\cdot b\cdot\cdots\cdot 3\cdot 2\cdot 1\end{aligned}$$

となり，b が $(a-1)!$ の約数となる．よって b は $(a-1)!+1$ の約数ではない．したがって，b の倍数である a は $(a-1)!+1$ の約数にはなれない．

例

$$\begin{aligned}(4-1)!+1 &= 3\cdot 2\cdot 1+1 = 7\\ &\equiv 3 \pmod 4\end{aligned}$$

$$(6-1)!+1 = 5\cdot 4\cdot 3\cdot 2\cdot 1+1 = 121$$
$$\equiv 1 \pmod 6. \text{ ——}$$

以上をまとめると，次の定理が得られる．

定理 11（ウィルソン）　2以上の自然数 a に対して，a が素数である必要十分条件は $(a-1)!+1$ が a で割れることである．——

§6　4つの平方数の和

この節ではどのような自然数 n も4つの平方数の和として表わされること，すなわち

$$n = a^2+b^2+c^2+d^2$$

となることを証明しよう．

例

$$1 = 1^2+0^2+0^2+0^2, \qquad 2 = 1^2+1^2+0^2+0^2,$$
$$3 = 1^2+1^2+1^2+0^2, \qquad 4 = 2^2+0^2+0^2+0^2,$$
$$5 = 2^2+1^2+0^2+0^2, \qquad 6 = 2^2+1^2+1^2+0^2,$$
$$7 = 2^2+1^2+1^2+1^2, \qquad 8 = 2^2+2^2+0^2+0^2,$$
$$9 = 3^2+0^2+0^2+0^2, \qquad 10 = 3^2+1^2+0^2+0^2. \text{ ——}$$

準備としてまず次の恒等式が成り立つことをみる．

(1)
$$\begin{aligned}&({x_1}^2+{x_2}^2+{x_3}^2+{x_4}^2)({y_1}^2+{y_2}^2+{y_3}^2+{y_4}^2)\\ &= (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2+(-x_1y_2+x_2y_1-x_3y_4+x_4y_3)^2\\ &\quad +(x_1y_3-x_2y_4-x_3y_1+x_4y_2)^2+(x_1y_4+x_2y_3-x_3y_2-x_4y_1)^2.\end{aligned}$$

両辺の掛け算をしてばらばらにすれば証明出来るけれど，複素数を利用すると計算が楽になる．複素数の性質をみておく．

$i=\sqrt{-1}$ とし，$\alpha=a+bi, \beta=c+di$ とおけば

(2)　$$\alpha+\beta = (a+c)+(b+d)i$$

(3)　$$\alpha-\beta = (a-c)+(b-d)i$$

(4)　$$\alpha\cdot\beta = (ac-bd)+(ad+bc)i$$

となる．$\gamma=e+fi$ に対し，その**共役**を $\bar{\gamma}=e-fi$ と定義する．つま

り虚数部の符号を逆にするわけである．このとき，(2)から

$$\begin{aligned}\bar\alpha+\bar\beta &= (a-bi)+(c-di)\\ &= (a+c)-(b+d)i\\ &= \overline{\alpha+\beta}\end{aligned}$$

となる．共役にしてから足しても，足してから共役にしても同じになる．同様に(3), (4)から

$$\begin{aligned}\bar\alpha-\bar\beta &= (a-bi)-(c-di)\\ &= (a-c)-(b-d)i\\ &= \overline{\alpha-\beta}\\ \bar\alpha\cdot\bar\beta &= (a-bi)\cdot(c-di)\\ &= (ac-bd)-(ad+bc)i\\ &= \overline{\alpha\cdot\beta}\end{aligned}$$

となる．また2回共役にすると

$$\bar{\bar\alpha} = \overline{a-bi} = a+bi = \alpha$$

となり元にもどる．これらのことから，たとえば

$$\begin{aligned}\overline{\alpha\bar\gamma+\beta\bar\delta} &= \overline{\alpha\bar\gamma}+\overline{\beta\bar\delta}\\ &= \bar\alpha\bar{\bar\gamma}+\bar\beta\bar{\bar\delta}\\ &= \bar\alpha\gamma+\bar\beta\delta\end{aligned}$$

となる．同様に計算すると

$$\begin{aligned}(5)\qquad &(\alpha\bar\gamma+\beta\bar\delta)(\overline{\alpha\bar\gamma+\beta\bar\delta})+(\alpha\delta-\beta\gamma)(\overline{\alpha\delta-\beta\gamma})\\ &= (\alpha\bar\gamma+\beta\bar\delta)(\bar\alpha\gamma+\bar\beta\delta)+(\alpha\delta-\beta\gamma)(\bar\alpha\bar\delta-\bar\beta\bar\gamma)\\ &= \alpha\bar\alpha\gamma\bar\gamma+\alpha\bar\beta\bar\gamma\delta+\bar\alpha\beta\gamma\bar\delta+\beta\bar\beta\delta\bar\delta\\ &\quad +\alpha\bar\alpha\delta\bar\delta-\alpha\bar\beta\bar\gamma\delta-\bar\alpha\beta\gamma\bar\delta+\beta\bar\beta\gamma\bar\gamma\\ &= \alpha\bar\alpha(\gamma\bar\gamma+\delta\bar\delta)+\beta\bar\beta(\gamma\bar\gamma+\delta\bar\delta)\\ &= (\alpha\bar\alpha+\beta\bar\beta)(\gamma\bar\gamma+\delta\bar\delta)\end{aligned}$$

となる．

さて(1)を得るには $\alpha, \beta, \gamma, \delta$ として

$$\alpha = x_1 + x_2 i, \quad \beta = x_3 + x_4 i, \quad \gamma = y_1 + y_2 i, \quad \delta = y_3 + y_4 i$$

とおく．或る複素数とその共役を掛ける，たとえば

$$\alpha\bar{\alpha} = (x_1 + x_2 i)(x_1 - x_2 i) = x_1^2 + x_2^2$$

となり，実部の平方と虚部の平方の和となる．よって(5)の右辺は

$$\begin{aligned}&(\alpha\bar{\alpha} + \beta\bar{\beta})(\gamma\bar{\gamma} + \delta\bar{\delta})\\ &\quad = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)\end{aligned}$$

となり(1)の左辺となる．(5)の左辺を計算するとまず

$$\begin{aligned}\alpha\bar{\gamma} + \beta\bar{\delta} &= (x_1 + x_2 i)(y_1 - y_2 i) + (x_3 + x_4 i)(y_3 - y_4 i)\\ &= (x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4)\\ &\quad + (-x_1 y_2 + x_2 y_1 - x_3 y_4 + x_4 y_3)i\\ \alpha\delta - \beta\gamma &= (x_1 + x_2 i)(y_3 + y_4 i) - (x_3 + x_4 i)(y_1 + y_2 i)\\ &= (x_1 y_3 - x_2 y_4 - x_3 y_1 + x_4 y_2)\\ &\quad + (x_1 y_4 + x_2 y_3 - x_3 y_2 - x_4 y_1)i\end{aligned}$$

となり，共役を作り，掛け，加えると(1)の右辺が得られる．以上で(1)が成り立つことがわかった．

この等式により，どのような素数も4つの平方数の和になることさえ示せばよい．n が m 個の素数の積ならば $m-1$ 回(1)を使えばよいからである．

例

$$\begin{aligned}21 &= 3 \cdot 7\\ &= (1^2 + 1^2 + 1^2 + 0^2)(2^2 + 1^2 + 1^2 + 1^2)\end{aligned}$$

であるから

$$x_1 = 1, \quad x_2 = 1, \quad x_3 = 1, \quad x_4 = 0,$$
$$y_1 = 2, \quad y_2 = 1, \quad y_3 = 1, \quad y_4 = 1$$

とおけば，(1)から

$$\begin{aligned}21 &= (1\cdot2 + 1\cdot1 + 1\cdot1 + 0\cdot1)^2 + (-1\cdot1 + 1\cdot2 - 1\cdot1 + 0\cdot1)^2\\ &\quad + (1\cdot1 - 1\cdot1 - 1\cdot2 + 0\cdot1)^2 + (1\cdot1 + 1\cdot1 - 1\cdot1 - 0\cdot2)^2\\ &= 4^2 + 0^2 + 2^2 + 1^2\end{aligned}$$

となる. ——

$p=2$ の場合は成り立っているから，以後，$p=$ 奇素数，とする．まず p^2 より小さな p の倍数で，4つの平方の和になっている数が存在することを証明しよう．それには

$$(6) \qquad 0^2,\ 1^2,\ 2^2,\ \cdots,\ \left(\frac{p-1}{2}\right)^2$$

という $(p+1)/2$ 個の平方数を考えよう．これらのどの2つも $\mathrm{mod}\, p$ で合同ではない．なぜならば

$$j^2 \equiv i^2 \pmod{p}, \qquad 0 \leqq i < j \leqq (p-1)/2$$

のとき $j^2-i^2=(j-i)(j+i)$ が p で割れる．$j-i$ は p で割れないから $j+i$ が p で割れなければいけない．ところが $0<j+i<(p-1)/2+(p-1)/2<p$ から $j+i$ は p で割れない．よって(6)のどの2つも $\mathrm{mod}\, p$ で不合同である．よってそれらを -1 から引いた数

$$(7) \qquad -1,\ -1-1^2,\ -1-2^2,\ \cdots,\ -1-\left(\frac{p-1}{2}\right)^2$$

も $\mathrm{mod}\, p$ で不合同である．(6)と(7)を合わせると全部で $p+1$ 個の数がある．よって部屋割り論法から $\mathrm{mod}\, p$ で考えれば，同じ類に入っている数がある．つまり

$$a^2 \equiv -1-b^2 \pmod{p}, \qquad 0 \leqq a,\ b \leqq (p-1)/2$$

となる整数 a と b がある．これは a^2+b^2+1 が p で割れることを意味する．つまり

$$ph = a^2+b^2+1, \qquad 0 \leqq a,\ b \leqq (p-1)/2$$

となる自然数 h が存在する．しかも

$$\begin{aligned} ph &= a^2+b^2+1 \\ &\leqq (p-1)^2/4+(p-1)^2/4+1 \\ &= (p-1)^2/2+1 \\ &< (p-1)^2/2+(p-1)^2/2 \end{aligned}$$

$$<p^2$$

であるから $1\leqq h<p$ である．つまり p^2 より小さな p の倍数で $a^2+b^2+1^2+0^2$ と4つの平方の和に書ける数が見つかったわけである．

さて $h=1$ ならば証明は終りである．$h>1$ ならば $h>r\geqq 1$ となる r で pr が4つの平方数の和となっているものを作り出そう．もしこのことが言えたら，$r=1$ ならば証明は終りだし，$r>1$ ならば同じ論法を用いてさらに小さくしていくことが出来，最後には p が4つの平方数の和となる．

さて一般に

(8) $$x_1{}^2+x_2{}^2+x_3{}^2+x_4{}^2=ph, \qquad 1<h<p$$

であったとする．x_i を h で割り

$$x_i=h\cdot q_i+r_i, \qquad 0\leqq r_i<h$$

としたとき，$0\leqq r_i\leqq h/2$ ならば $y_i=r_i$ とおき，$h/2<r_i<h$ ならば h を引き $-h/2<r_i-h<0$ となるので $y_i=r_i-h$ とおくと

(9) $$x_i\equiv y_i \pmod h, \qquad -h/2<y_i\leqq h/2$$

となる y_i $(i=1,2,3,4)$ は定まる．このとき

$$\begin{aligned} y_1{}^2+y_2{}^2+y_3{}^2+y_4{}^2 &\equiv x_1{}^2+x_2{}^2+x_3{}^2+x_4{}^2 \\ &\equiv 0 \pmod h \end{aligned}$$

となるので

(10) $$y_1{}^2+y_2{}^2+y_3{}^2+y_4{}^2=hr$$

となる r が定まる．このとき(1)を利用して

$$\begin{aligned} z_1 &= x_1y_1+x_2y_2+x_3y_3+x_4y_4 \\ z_2 &= -x_1y_2+x_2y_1-x_3y_4+x_4y_3 \\ z_3 &= x_1y_3-x_3y_1-x_2y_4+x_4y_2 \\ z_4 &= x_1y_4-x_4y_1+x_2y_3-x_3y_2 \end{aligned}$$

とおくと

(11) $$z_1{}^2+z_2{}^2+z_3{}^2+z_4{}^2$$

$$= (x_1{}^2+x_2{}^2+x_3{}^2+x_4{}^2)(y_1{}^2+y_2{}^2+y_3{}^2+y_4{}^2)$$
$$= ph\cdot hr = ph^2r$$

となる．また z_i を $\bmod h$ で考えると(9)から

$$z_1 \equiv x_1{}^2+x_2{}^2+x_3{}^2+x_4{}^2 = ph \equiv 0$$
$$z_2 \equiv -x_1x_2+x_2x_1-x_3x_4+x_4x_3 = 0$$
$$z_3 \equiv x_1x_3-x_3x_1-x_2x_4+x_4x_2 = 0$$
$$z_4 \equiv x_1x_4-x_4x_1+x_2x_3-x_3x_2 = 0$$

となり z_i は h で割り切れる．よって

$$z_1 = ht_1, \quad z_2 = ht_2, \quad z_3 = ht_3, \quad z_4 = ht_4$$

とおき(11)の両辺を h^2 で割ると

(12)　$$t_1{}^2+t_2{}^2+t_3{}^2+t_4{}^2 = pr$$

となる．さて $1\leqq r<h$ を示そう．(9)から

$$hr = y_1{}^2+y_2{}^2+y_3{}^2+y_4{}^2 \leqq 4(h/2)^2 = h^2$$

となり $r\leqq h$ が得られる．もし $r=h$ ならば

$$y_1 = y_2 = y_3 = y_4 = h/2$$

でなければならない．よって h は偶数となり，(9)から x_i は $h/2$ の奇数倍となる．

$$x_i = (2m_i+1)\cdot h/2 \qquad (i=1, 2, 3, 4)$$

とおけば

$$x_1{}^2+x_2{}^2+x_3{}^2+x_4{}^2$$
$$= \{(2m_1+1)^2+(2m_2+1)^2+(2m_3+1)^2+(2m_4+1)^2\}\cdot h^2/4$$
$$= (4m_1{}^2+4m_1+1+4m_2{}^2+4m_2+1+4m_3{}^2+4m_3+1$$
$$+4m_4{}^2+4m_4+1)\cdot h^2/4$$
$$= (m_1{}^2+m_1+m_2{}^2+m_2+m_3{}^2+m_3+m_4{}^2+m_4+1)\cdot h^2$$

となる．この値が(8)から ph であるから，両辺を h で割ると

$$p = (m_1{}^2+m_1+m_2{}^2+m_2+m_3{}^2+m_3+m_4{}^2+m_4+1)\cdot h$$

となる．h は偶数であるから矛盾である．よって $r<h$ が得られた．

次に $r \neq 0$ を示そう.

もし $r=0$ とすると(10)から $y_1=y_2=y_3=y_4=0$ となる. よって(9)から

$$x_1 = hu_1, \quad x_2 = hu_2, \quad x_3 = hu_3, \quad x_4 = hu_4$$

となる u_i が定まる. このとき(8)の両辺を h^2 で割り

$$u_1{}^2+u_2{}^2+u_3{}^2+u_4{}^2 = p/h, \quad 1 < h < p$$

となる. しかし右辺は整数でないから矛盾である. よって(12)と $1 \leqq r < h$ が得られ, 証明が完成した. まとめると

定理 12 どのような自然数も4つの平方数の和に表わすことが出来る. ただし, 平方数の中に0の平方, つまり0も含める. ——

第6章　原　始　根

いろいろな合同式を解くとき，原始根を利用すると，うまくゆく場合が多い．原始根はすべての数を作り出す力を持っている．たとえばpを奇数とすると，pの原始根と呼ばれる特別の整数rが存在して

$$1,\ 2,\ 3,\ \cdots,\ p-1$$

と

$$r,\ r^2,\ r^3,\ \cdots,\ r^{p-1}$$

は$\bmod p$で考えると，全体として等しくなる．よってpの倍数以外のどのような数も，rの或る巾と$\bmod p$で合同となる．この性質を利用すると，さまざまな問題が見通し良く解ける．この章では原始根が存在することの証明と，原始根を利用して，4で割れば1余るどのような素数も，2つの平方数の和として表わされることを示そう．準備としてオイラー関数を定義し，オイラーの定理とフェルマーの定理を証明しよう．フェルマーの定理は初等整数論で良く用いられる便利な定理である．

§1　オイラー関数

自然数nに対して

$$1,\ 2,\ \cdots,\ n$$

の中でnと互いに素な数の個数を$\varphi(n)$と表わす．この関数のことを**オイラー関数**という．たとえば$n=5$のとき

$$1,\ 2,\ 3,\ 4,\ 5$$

の中で，5と互いに素な数は$1, 2, 3, 4$であるから$\varphi(5)=4$となる．n

$=12$ のとき

$$1,\ 2,\ 3,\ \cdots,\ 12$$

の中で 12 と互いに素な数とは，2 や 3 で割れない数，すなわち 1, 5, 7, 11 であるから $\varphi(12)=4$ となる．

例　$1\leqq n\leqq 10$ までの $\varphi(n)$ の表を作れ．

解　n と互いに素な数をならべると，次のようになる．$n=1$ のとき，1 と 1 は互いに素であることに注意しよう．

表 6–1

n	n と互いに素な数	$\varphi(n)$
1	1	1
2	1	1
3	1, 2	2
4	1, 3	2
5	1, 2, 3, 4	4
6	1, 5	2
7	1, 2, 3, 4, 5, 6	6
8	1, 3, 5, 7	4
9	1, 2, 4, 5, 7, 8	6
10	1, 3, 7, 9	4

——

素数 p に対して

$$1,\ 2,\ 3,\ \cdots,\ p$$

の中で，p と互いに素な数は p 以外の

$$1,\ 2,\ 3,\ \cdots,\ p-1$$

であるから

$$\varphi(p)=p-1$$

となる．n が素数の巾 p^m のときは

$$1,\ 2,\ 3,\ \cdots,\ p^m$$

の中で p^m と互いに素な数とは，つまり p で割れない数である．逆

に p で割れる数は

$$p,\ 2p,\ \cdots,\ p^{m-1}\cdot p$$

と p^{m-1} 個ある．これらの数以外が p^m と互いに素な数であるから

$$\varphi(p^m) = p^m - p^{m-1}$$
$$= p^m\left(1-\frac{1}{p}\right)$$

となる．$n=p_1{}^e\cdot p_2{}^f$ のとき，つまり 2 つの素数で割れるとき

$$1,\ 2,\ \cdots,\ p_1{}^e\cdot p_2{}^f$$

の中で n と互いに素でない数とは p_1 または p_2 で割れる数である．つまり

(1)　$$p_1,\ 2p_1,\ 3p_1,\ \cdots,\ \frac{n}{p_1}\cdot p_1$$

または

(2)　$$p_2,\ 2p_2,\ 3p_2,\ \cdots,\ \frac{n}{p_2}\cdot p_2$$

である．これらの $\dfrac{n}{p_1}$ 個と $\dfrac{n}{p_2}$ 個をぬかせば，のこりは n と互いに素な数である．しかし(1)と(2)の両方に現われる数もある．それらの数はだぶってぬかされてしまう．それらは p_1p_2 の倍数

$$p_1p_2,\ 2p_1p_2,\ \cdots,\ \frac{n}{p_1p_2}\cdot p_1p_2$$

の $\dfrac{n}{p_1p_2}$ 個の数である．よって

$$\varphi(n) = n-\frac{n}{p_1}-\frac{n}{p_2}+\frac{n}{p_1p_2}$$
$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)$$

となる．たとえば $n=12=2^2\cdot 3$ のとき

$$\varphi(12) = 12\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)$$

$$= 4$$

となる.

一般に $n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ のとき

(3) $$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

となることを証明しよう. そのために n が少なくとも i 個の素数 $p_1, p_2, \cdots, p_i$ で割れるとき

(4) $$1,\ 2,\ \cdots,\ n$$

の中で $p_1, p_2, \cdots, p_i$ と互いに素な数の個数を $\varphi_i(n)$ と表わし,

(5) $$\varphi_i(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_i}\right)$$

となることを帰納法を用い証明しよう. もし(5)が正しければ $i=r$ のとき $\varphi_r(n)=\varphi(n)$ であるから, (5)から(3)が導かれるわけである.

さて $i=1$ のとき, (4)の中で p_1 と互いに素な数の個数を数えよう. p_1 と互いに素でない数とは p_1 の倍数

$$p_1,\ 2p_1,\ \cdots,\ \frac{n}{p_1}\cdot p_1$$

であるから, これら以外が p_1 と互いに素となる. よって

$$\varphi_1(n) = n-\frac{n}{p_1}$$
$$= n\left(1-\frac{1}{p_1}\right)$$

となり, $i=1$ の場合が証明された. i まで正しいとして, $i+1$ の場合を考えよう. そのために $\varphi_i(n)-\varphi_{i+1}(n)$ の値を考えよう. この値は $p_1, p_2, \cdots, p_i$ と互いに素である数の個数から, $p_1, p_2, \cdots, p_{i+1}$ と互いに素である数の個数を引いたものである. つまり $p_1, p_2, \cdots, p_i$ と互いに素であるが, p_{i+1} で割り切れる数の個数である. p_{i+1} で割り切れる数とは

$$p_{i+1},\ \ 2p_{i+1},\ \ \cdots,\ \ \frac{n}{p_{i+1}}\cdot p_{i+1}$$

である．この中で $p_1, p_2, \cdots, p_i$ と互いに素な数の個数は

$$(6)\qquad 1,\ 2,\ \cdots,\ \frac{n}{p_{i+1}}$$

の中で $p_1, p_2, \cdots, p_i$ と互いに素な数の個数と等しい．p_{i+1} で割ってもも $p_1, p_2, \cdots, p_i$ と互いに素か，否かという関係は変わらないからである．

(6) の中で $p_1, p_2, \cdots, p_i$ と互いに素な数の個数は $\varphi_i\left(\dfrac{n}{p_{i+1}}\right)$ であり，i に関する帰納法から

$$(7)\qquad \varphi_i\left(\frac{n}{p_{i+1}}\right)=\frac{n}{p_{i+1}}\cdot\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_i}\right)$$

となる．n の代りに $\dfrac{n}{p_{i+1}}$ を使っているところが気になるが，n が少なくとも i 個の素数 $p_1, \cdots, p_i$ で割れるとき，(4) の中で $p_1, \cdots, p_i$ と互いに素となる数の個数が (5) で表わされることを証明しているのであり，$\dfrac{n}{p_{i+1}}$ は少なくとも $p_1, \cdots, p_i$ で割れるから，n の代りに $\dfrac{n}{p_{i+1}}$ を使ってもよいわけである．

(7) の値が $\varphi_i(n)-\varphi_{i+1}(n)$ であるから

$$\begin{aligned}\varphi_{i+1}(n) &= \varphi_i(n)-(\varphi_i(n)-\varphi_{i+1}(n))\\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_i}\right)\\ &\quad -\frac{n}{p_{i+1}}\cdot\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_i}\right)\\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_{i+1}}\right)\end{aligned}$$

から (5) が $i+1$ の場合について示された．よって帰納法からいつでも (5) が成立する．まとめると次のようになる．

定理 13 $1, 2, \cdots, n$ の中で n と素な数の個数を $\varphi(n)$ とすると

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_r^{e_r}$$

ならば

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

となる. ——

例 $\varphi(1001)$ を求めよ.

解 $1001 = 7\times11\times13$ であるから

$$\begin{aligned}\varphi(1001) &= 1001\cdot\left(1-\frac{1}{7}\right)\left(1-\frac{1}{11}\right)\left(1-\frac{1}{13}\right) \\ &= 6\times10\times12 \\ &= 720.\end{aligned}$$ ——

a が b の約数のとき $a|b$ と書く(**ランダウの記号**). 左側が約数で, 右側が倍数である. たとえば $5|10$ である. この記号は使いなれると便利である.

さてオイラー関数 $\varphi(n)$ に対して

(8) $$\sum_{d|n}\varphi(d) = n$$

が成り立つ. 和の意味は, $d|n$ となるすべての d に対しての和, つまり n のすべての約数 d に対しての和である.

例 $n=12$ のとき $d=1, 2, 3, 4, 6, 12$ と動き

$$\begin{aligned}&\varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\varphi(12) \\ &= 1+1+2+2+2+4 = 12 = n.\end{aligned}$$ ——

(8) の証明は次のようになる.

d を n の1つの約数とする.

$$1,\ 2,\ \cdots,\ n$$

のうち n との最大公約数が d となる x は $x=x_1\cdot d$, と書け, $n=d_1\cdot d$ とおいたとき $(x_1, d_1)=1$ の場合である. つまり x_1 は

$$d,\ 2d,\ 3d,\ \cdots,\ d_1d = n$$

を d で割った

$$1,\ 2,\ 3,\ \cdots,\ d_1$$

のうち d_1 と互いに素になる数である．よって $\varphi(d_1)$ 個ある，$1, 2, \cdots,$ n のどの数も，n との最大公約数が n の約数になるから $n=\sum_{d|n}\varphi(d_1)$ となる．

例　$n=12$ のとき，$d=1, 2, 3, 4, 6, 12$ となり $\varphi(d_1)$ を加えると，1 から 12 までの数の個数，つまり 12 となる．

表 6-2

$d=(x, n)$	x	$\varphi(d_1)$
1	1, 5, 7, 11	$\varphi(12)=4$
2	2, 10	$\varphi(6)=2$
3	3, 9	$\varphi(4)=2$
4	4, 8	$\varphi(3)=2$
6	6	$\varphi(2)=1$
12	12	$\varphi(1)=1$

——

さて $n=d_1d$ であり，d が n の約数全部を 1 回ずつ動けば，d_1 も n の約数を 1 回ずつ動く．よって

$$\sum_{d|n}\varphi(d_1)=\sum_{d_1|n}\varphi(d_1)=\sum_{d|n}\varphi(d)$$

となり (8) が示された．まとめると次の定理が得られる．

定理 14　n のすべての約数 d についての $\varphi(d)$ の和は n となる．つまり

$$\sum_{d|n}\varphi(d)=n$$

となる．——

§2　フェルマーの定理

2 以上の自然数 n に対して，$1\leqq a\leqq n, (a, n)=1$ となる a は $\varphi(n)$ 個ある．それらを

(1) $$a_1,\ a_2,\ \cdots,\ a_{\varphi(n)}$$

とする．$(b, n)=1$ となる b に対して b を n で割った余りを a とする．つまり $b=n\cdot q+a$ $(0\leqq a<n)$ とする．もし $(a, n)=d>1$ ならば d は n および a を割るから b も割る．しかし $(b, n)=1$ であるから $(a, n)=1$ でなければならない．つまり a は(1)の中のどれかである．さて(1)の中から1つ a_i を取り出すと，$(b, n)=1, (a_i, n)=1$ から $(b\cdot a_i, n)=1$ となる．よって $b\cdot a_i$ を n で割った余りは(1)の中にある．それを a_i' と書けば $b\cdot a_i\equiv a_i' \pmod n$ となる．(1)の中からもう1つの数 a_j を取り出したとき，$ba_i\equiv ba_j \pmod n$ とはならない．なぜなら，もし $ba_i\equiv ba_j$ ならば $ba_i-ba_j=b(a_i-a_j)$ が n で割れる．$(b, n)=1$ であるから a_i-a_j が n で割れる．$-n<a_i-a_j<n$ であるから a_i-a_j が n で割れるとは $a_i=a_j$ を意味する．よって $a_i\neq a_j$ ならば $ba_i\not\equiv ba_j \pmod n$ となり ba_j を n で割った余りを a_j' とおくと $a_i'\neq a_j'$ となる．

さて i を1から $\varphi(n)$ まで動かしたとき，$ba_i\equiv a_i' \pmod n$ となる a_i' は(1)の中の数ではあるが，i が異なれば a_i' も異なるから，$\varphi(n)$ 通りの数が現われる．(1)は $\varphi(n)$ 個しかなく，その中で $\varphi(n)$ 通りの数が現われるということはすべてが現われる，ということである．

例 m 個の部屋のあるホテルに m 人の人が泊っている．1部屋に1人しか泊っていないとしたら，全部の部屋はふさがっている．

――

この論法は部屋割り論法と異なるが，しかし，それに劣らず大切である．この論法により i を1から $\varphi(n)$ まで動かしたとき，順はかわるが a_i' は(1)のすべてを1回ずつ取るわけである．$b\cdot a_i\equiv a_i'$ であるからすべての積を作ると

$$\begin{aligned} ba_1\cdot ba_2\cdot\cdots\cdot ba_{\varphi(n)} &\equiv a_1'\cdot a_2'\cdot\cdots\cdot a_{\varphi(n)}' \pmod n \\ &= a_1\cdot a_2\cdot\cdots\cdot a_{\varphi(n)} \end{aligned}$$

となる．b をまとめると

$$b^{\varphi(n)}\cdot(a_1a_2\cdots a_{\varphi(n)}) \equiv a_1a_2\cdots a_{\varphi(n)} \pmod n$$

となり，$(a_i, n)=1$ から $(a_1a_2\cdots a_{\varphi(n)}, n)=1$ であるから，両辺を $a_1a_2\cdots a_{\varphi(n)}$ で割ると

$$b^{\varphi(n)} \equiv 1 \pmod n \tag{2}$$

が得られる．これを**オイラーの定理**という．n が素数 p のときは $\varphi(p)=p-1$ であるから

$$(b, p)=1 \quad \text{ならば} \quad b^{p-1} \equiv 1 \pmod p \tag{3}$$

が得られる．これを**フェルマーの定理**という．フェルマーの大定理と区別するためにフェルマーの小定理ということもある．まとめると次のようになる．

定理 15　a が n と素ならば，つまり $(a, n)=1$ ならば

$$a^{\varphi(n)} \equiv 1 \pmod n$$

となる．特に $n=p=$素数ならば

$$a^{p-1} \equiv 1 \pmod p$$

となる．――

例　$b=2$ の場合に 2^{p-1} を計算してみよう．

$$2^{3-1} = 4 = 3\cdot1+1$$
$$2^{5-1} = 16 = 5\cdot3+1$$
$$2^{7-1} = 64 = 7\cdot9+1$$
$$2^{11-1} = 1024 = 11\cdot93+1$$
$$2^{13-1} = 4096 = 13\cdot315+1$$
$$2^{17-1} = 65536 = 17\cdot3855+1$$
$$2^{19-1} = 262144 = 19\cdot13797+1$$
$$2^{23-1} = 4194304 = 23\cdot182361+1$$
$$2^{29-1} = 268435456 = 29\cdot9256395+1$$
$$2^{31-1} = 1073741824 = 31\cdot34636833+1$$

$$2^{37-1} = 68719476736 = 37 \cdot 1857283155 + 1$$
$$2^{41-1} = 1099511627776 = 41 \cdot 26817356775 + 1$$
$$2^{43-1} = 4398046511104 = 43 \cdot 102280151421 + 1$$
$$2^{47-1} = 70368744177664 = 47 \cdot 1497207322929 + 1$$

となり，$2^{p-1}-1$ はいつも p で割れる．——

例　$2^{p-1}-1$ は p^2 で割れるだろうか．

解
$$(2^{3-1}-1)/3 = 1 = 3 \cdot 0 + 1$$
$$(2^{5-1}-1)/5 = 3 = 5 \cdot 0 + 3$$
$$(2^{7-1}-1)/7 = 9 = 7 \cdot 1 + 2$$
$$(2^{11-1}-1)/11 = 93 = 11 \cdot 8 + 5$$
$$(2^{13-1}-1)/13 = 315 = 13 \cdot 24 + 3$$
$$(2^{17-1}-1)/17 = 3855 = 17 \cdot 226 + 13$$
$$(2^{19-1}-1)/19 = 13797 = 19 \cdot 726 + 3$$
$$(2^{23-1}-1)/23 = 182361 = 23 \cdot 7928 + 17$$
$$(2^{29-1}-1)/29 = 9256395 = 29 \cdot 319186 + 1$$
$$(2^{31-1}-1)/31 = 34636833 = 31 \cdot 1117317 + 6$$
$$(2^{37-1}-1)/37 = 1857283155 = 37 \cdot 50196842 + 1$$
$$(2^{41-1}-1)/41 = 26817356775 = 41 \cdot 654081872 + 23$$
$$(2^{43-1}-1)/43 = 102280151421 = 43 \cdot 2378608172 + 25$$
$$(2^{47-1}-1)/47 = 1497207322929 = 47 \cdot 31855474955 + 44$$

となり $2^{p-1} \equiv 1 \pmod{p^2}$ となる素数は見つからない．——

実は $2^{p-1} \equiv 1 \pmod{p^2}$ となる最小の素数は 1093 である．

例　$p=1093$ のとき，$2^{p-1} \equiv 1 \pmod{p^2}$ を示せ．

解　3^7 を計算すると 2187 となる．よって

$$3^7 = 2187 = 2p+1.$$

両辺を自乗して

$$3^{14} = (2p+1)^2 \equiv 4p+1 \pmod{p^2}. \tag{4}$$

2^{14} を計算すると 16384 となる．よって

$$2^{14}=16384=15p-11.$$

両辺を自乗して

$$2^{28}\equiv -330p+121 \pmod{p^2}.$$

よって $3^2, 3^2\cdot 7$ を掛けると

$$\begin{aligned}3^2\cdot 2^{28} &\equiv -9\cdot 330p+9\cdot 121 \pmod{p^2}\\ &\equiv 309p+(p-4) \pmod{p^2}\\ &= 310p-4\\ 3^2\cdot 2^{28}\cdot 7 &\equiv 2170p-28 \pmod{p^2}\\ &\equiv -16p-28 \pmod{p^2}\\ &= 4(-4p-7).\end{aligned}$$

両辺を 4 で割り，7 乗すると

$$\begin{aligned}3^2\cdot 2^{26}\cdot 7 &\equiv -4p-7 \pmod{p^2}\\ 3^{14}\cdot 2^{182}\cdot 7^7 &\equiv -(4p+7)^7 \pmod{p^2}\\ &\equiv -7\cdot 4p\cdot 7^6-7^7 \pmod{p^2}\\ &= 7^7(-4p-1).\end{aligned}$$

両辺を 7^7 で割り，(4) を利用すると

$$\begin{aligned}3^{14}\cdot 2^{182} &\equiv -4p-1 \pmod{p^2}\\ &\equiv -3^{14} \pmod{p^2}.\end{aligned}$$

両辺を 3^{14} で割り，6 乗すると

$$2^{182}\equiv -1 \pmod{p^2}$$

$$2^{1092}\equiv 1 \pmod{p^2}. \text{———}$$

現在のところ $p<3\times 10^9$ の範囲で 1093 と 3511 の 2 つしか $2^{p-1}\equiv 1 \pmod{p^2}$ を満たさないことがわかっている．

例 $b=3$ の場合に，3^{p-1} を計算してみよう．

$3^{2-1}=3=2\cdot 1+1$

$3^{5-1}=81=5\cdot 16+1$

$$3^{7-1} = 729 = 7\cdot 104+1$$
$$3^{11-1} = 59049 = 11\cdot 5368+1$$
$$3^{13-1} = 531441 = 13\cdot 40880+1$$
$$3^{17-1} = 43046721 = 17\cdot 2532160+1$$
$$3^{19-1} = 387420489 = 19\cdot 20390552+1$$
$$3^{23-1} = 31381059609 = 23\cdot 1364393896+1$$
$$3^{29-1} = 22876792454961 = 29\cdot 788854912240+1$$
$$3^{31-1} = 205891132094649 = 31\cdot 6641649422408+1$$
$$3^{37-1} = 150094635296999121 = 37\cdot 4056611764783760+1$$
$$3^{41-1} = 12157665459056928801$$
$$= 41\cdot 296528425830656800+1$$

となり，$3^{p-1}-1$ はいつも p で割り切れる．——

例 $3^{p-1}-1$ は p^2 で割れるだろうか．

解
$$(3^{2-1}-1)/2 = 1 = 2\cdot 0+1$$
$$(3^{5-1}-1)/5 = 16 = 5\cdot 3+1$$
$$(3^{7-1}-1)/7 = 104 = 7\cdot 14+6$$
$$(3^{11-1}-1)/11 = 5368 = 11\cdot 488+0$$
$$(3^{13-1}-1)/13 = 40880 = 13\cdot 3144+8$$
$$(3^{17-1}-1)/17 = 2532160 = 17\cdot 148950+10$$
$$(3^{19-1}-1)/19 = 20390552 = 19\cdot 1073186+18$$
$$(3^{23-1}-1)/23 = 1364393896 = 23\cdot 59321473+17$$
$$(3^{29-1}-1)/29 = 788854912240 = 29\cdot 27201893525+15$$
$$(3^{31-1}-1)/31 = 6641649422408 = 31\cdot 214246755561+17$$
$$(3^{37-1}-1)/37 = 4056611764783760$$
$$= 37\cdot 109638155804966+18$$
$$(3^{41-1}-1)/41 = 296528425830656800$$
$$= 41\cdot 7232400630016019+21$$

となり $p=11$ のみが $3^{p-1}\equiv 1 \pmod{p^2}$ を満たす．——

実は $p<10^7$ ならば $p=11, 1006003$ のみが $3^{p-1}\equiv 1 \pmod{p^2}$ を満たすことが知られている．

§3　フェルマーテストと2進法

フェルマーの定理から，$(a, n)=1$ のとき

$$n = \text{素数} \quad \text{ならば} \quad a^{n-1} \equiv 1 \pmod{n}$$

となる．この対偶を取れば

$$a^{n-1} \not\equiv 1 \pmod{n} \quad \text{ならば} \quad n \neq \text{素数}$$

となる．これを**フェルマーテスト**という．

例　$a=2, n=15$ のとき

$$2^{14} = 16384 \equiv 4 \pmod{15}$$

であるから，15は素数でない．——

この例の場合，15が素数でないことを示すために，2^{14} を計算するのはずいぶん無駄の多いテストだと思うであろう．しかし n がたとえ100桁くらいの大きな数であっても，次に説明するように計算すれば a^{n-1} は計算機を利用し容易に計算出来る．

まず，平方を繰り返し

(1)　$$a^2,\ a^4,\ a^8,\ a^{16},\ \cdots,\ a^{2^m} = (a^{2^{m-1}})^2$$

を計算する．m は

$$2^m \leqq n-1 < 2^{m+1}$$

で定まる数である．(1)のいくつかを掛け合わせれば a^{n-1} が得られる．目的は a^{n-1} が mod n でいくつになるか，ということだから，(1)の中で n より大きいものが現われたとき，n で割った余りでおきかえてよい．

例　$a=2, n=101$ のとき，a^{n-1} を mod 101 で計算すると

$$a^2 = 4$$

$$\begin{aligned} a^4 &= (a^2)^2 = 4^2 = 16 \\ a^8 &= (a^4)^2 = 16^2 = 256 \equiv 54 \\ a^{16} &= (a^8)^2 \equiv 54^2 = 2916 \equiv 88 \\ a^{32} &= (a^{16})^2 \equiv 88^2 = 7744 \equiv 68 \\ a^{64} &= (a^{32})^2 \equiv 68^2 = 4624 \equiv 79 \\ 100 &= 64+32+4 \\ a^{100} &\equiv 79\cdot 68\cdot 16 \\ &= 85952 \\ &\equiv 1. \end{aligned}$$

101は素数であるから，この結果は当然である．——

この例の場合，100を

$$\begin{aligned} 100 &= 64+32+4 \\ &= 2^6+2^5+2^2 \end{aligned}$$

と分解した．このように分解することを**2進法**で表わすという．どのような自然数も2進法で表わすことができる．

例

$$\begin{aligned} &1 = 2^0, && 2 = 2^1, \\ &3 = 2+1, && 4 = 2^2, \\ &5 = 2^2+1, && 6 = 2^2+2, \\ &7 = 2^2+2+1, && 8 = 2^3, \\ &9 = 2^3+1, && 10 = 2^3+2. \end{aligned}$$

——

一般にbがどのように大きくとも

$$2^m \leqq b < 2^{m+1}$$

となるmは求まる．2^mを引くと

$$0 \leqq b-2^m < 2^{m+1}-2^m = 2^m$$

となる．$b-2^m>0$ならば同じように

$$2^{m_1} \leqq b-2^m < 2^{m_1+1} \qquad (0 \leqq m_1 < m)$$

となるm_1が見つかる．同様に続けていけば

$$b = 2^m + 2^{m_1} + 2^{m_2} + \cdots \qquad (m > m_1 > m_2 > \cdots)$$

となる．これを

$$(2) \qquad b = \sum_{i=0}^{m} a_i \cdot 2^{m-i} \qquad (a_i = 0 \text{ または } 1)$$

$$= a_0 a_1 a_2 \cdots a_m$$

と書く．これで２進法で表わすことの出来る証明が終った．次に b を与えたとき，能率よく a_i を計算する方法を考えよう．

$$b = a_0 \cdot 2^m + a_1 \cdot 2^{m-1} + \cdots + a_{m-1} \cdot 2 + a_m$$

$$= 2(a_0 2^{m-1} + a_1 2^{m-2} + \cdots + a_{m-1}) + a_m$$

であるから a_m は b を２で割った余りとして定まる．

$$b_1 = a_0 2^{m-1} + a_1 2^{m-2} + \cdots + a_{m-1}$$

とおくと，a_{m-1} は b_1 を２で割った余りとして定まる．このように順に $a_m, a_{m-1}, \cdots, a_0$ が求まる．特に(2)のような表わし方が１通りであることが示された．

例　$b=100$ のとき，この b を２進法で表わせ．

解

$$100 = 2 \cdot 50 + 0$$

$$50 = 2 \cdot 25 + 0$$

$$25 = 2 \cdot 12 + 1$$

$$12 = 2 \cdot 6 + 0$$

$$6 = 2 \cdot 3 + 0$$

$$3 = 2 \cdot 1 + 1$$

であるから

$$100 = 2^6 + 2^5 + 2^2$$

$$\therefore \quad 100 = 1100100.$$

左辺は10進法での表現であり，右辺は２進法での表現である．

さて，b が２進法で表わされているとき，10進法で書き直すにはどうしたらよいだろうか．$2^2, 2^3, \cdots$ の表を作っておけばよいが，次

のようにすると速く計算出来る.

まず a_0 らか出発し，2を掛け a_1 を加えると

$$a_0 \cdot 2 + a_1$$

となる．この値に2を掛け a_2 を加えると

$$(a_0 \cdot 2 + a_1) \cdot 2 + a_2 = a_0 \cdot 2^2 + a_1 \cdot 2 + a_2$$

となる．同様に繰り返すと最後に

$$\begin{aligned}(a_0 \cdot 2^{m-1} + a_1 \cdot 2^{m-2} + \cdots + a_{m-1}) \cdot 2 + a_m \\ = a_0 \cdot 2^m + a_1 \cdot 2^{m-1} + \cdots + a_{m-1} \cdot 2 + a_m\end{aligned}$$

が得られる.

例　2進法の1100100を10進法に直すと

$$\begin{aligned} 1 &= 1 \\ 1 \times 2 + 1 &= 3 \\ 3 \times 2 + 0 &= 6 \\ 6 \times 2 + 0 &= 12 \\ 12 \times 2 + 1 &= 25 \\ 25 \times 2 + 0 &= 50 \\ 50 \times 2 + 0 &= 100 \end{aligned}$$

となり100が得られる. ——

さて b が2進法で(2)のように表わされているとき，a^b を求めるには次のようにする.

まず a^{a_0} から出発し，自乗し，a^{a_1} を掛けると

$$(a^{a_0})^2 \cdot a^{a_1} = a^{a_0 \cdot 2 + a_1}$$

となる．この値を自乗し，a^{a_2} を掛けると

$$(a^{a_0 \cdot 2 + a_1})^2 \cdot a^{a_2} = a^{a_0 \cdot 2^2 + a_1 \cdot 2 + a_2}$$

となる．同様にして a^b が得られる.

例　2^{100} を mod 101 で計算せよ.

解　100を2進法で表わすと1100100であるから

$$2^2 \cdot 2 = 8$$
$$8^2 \cdot 1 = 64$$
$$64^2 \cdot 1 = 4096 \equiv 56$$
$$56^2 \cdot 2 = 6272 \equiv 10$$
$$10^2 \cdot 1 = 100 \equiv -1$$
$$(-1)^2 \cdot 1 = 1.$$

よって $2^{100} \equiv 1 \pmod{101}$ が得られた. ——

フェルマーの定理の逆は一般には正しくない. つまり $(b, n)=1$ のとき, いつも $b^{n-1} \equiv 1 \pmod{n}$ が成立しても, n=素数とはかぎらない.

例　$n=561=3 \cdot 11 \cdot 17$ のとき, $(a, n)=1$ ならば $(a, 3)=1, (a, 11)=1, (a, 17)=1$ となるのでフェルマーの定理から

$$a^2 \equiv 1 \pmod{3}$$
$$a^{10} \equiv 1 \pmod{11}$$
$$a^{16} \equiv 1 \pmod{17}$$

となる. $560=2 \cdot 280=10 \cdot 56=16 \cdot 35$ であるから

$$a^{560} = (a^2)^{280} \equiv 1 \pmod{3}$$
$$a^{560} = (a^{10})^{56} \equiv 1 \pmod{11}$$
$$a^{560} = (a^{16})^{35} \equiv 1 \pmod{17}$$

となる. よって $a^{560}-1$ は 3, 11, 17 を約数に持つ. よってその積 561 でも割れる. つまり

$$a^{n-1} \equiv 1 \pmod{n}$$

が $(a, n)=1$ となるすべての a に対して成り立つ. しかし 561 は素数ではない. ——

§4 原始根

2 以上の自然数 n と $(a, n)=1$ となる整数 a に対してオイラーの定

理から $a^{\varphi(n)}\equiv 1 \pmod{n}$ となる．しかし $\varphi(n)$ 乗しなくとも1と合同になることもある．

例 $n=7, a=2$ のとき

$$2^3=8\equiv 1 \pmod{7}$$

となり，3は $\varphi(7)=6$ より小さい．——

(1) $$a^l\equiv 1 \pmod{n}$$

となる自然数 l のうちで最小の数 e を，a の法 n に関する**位数**という．一般に(1)が成り立てば，l は e の倍数である．なぜならば $l=e\cdot q+r, 0\leqq r<e$ とすると $a^e\equiv 1$ であるから

$$a^r\equiv a^r\cdot(a^e)^q=a^{eq+r}=a^l\equiv 1 \pmod{n}$$

となり，e の最小性から $r=0$ でなければならない．特に $\varphi(n)$ は e の倍数である．

例 $n=7, a=2$ のとき mod 7 で考えると

$$a=2,\qquad a^2=4,\qquad a^3=8\equiv 1$$

であるから，2の法7に関する位数は3である．3は $\varphi(7)=6$ の約数である．——

a の法 n に関する位数が e のとき

(2) $$1,\ a,\ a^2,\ \cdots,\ a^{e-1}$$

は mod n で不合同である．なぜなら

$$a^i\equiv a^j \pmod{n}\qquad (0\leqq i<j<e)$$

ならば $(a^i, n)=1$ から両辺を a^i で割ることが出来

$$a^{j-i}\equiv 1 \pmod{n}\qquad (0<j-i<e)$$

が得られ，e の最小性に反する．

特に $n=$素数$=p$ の場合を考えよう．(2)のどの数も $(a^i)^e=(a^e)^i\equiv 1^i=1 \pmod{p}$ であるから

(3) $$x^e-1\equiv 0 \pmod{p}$$

の解である．ところが定理10からこの e 次式は多くとも e 個しか

解を持たないから，(3)の解のすべては(2)で尽される.

さて$(i, e)=d>1$ならば$i=d\cdot i_1$，$e=d\cdot e_1$とおくと

$$(a^i)^{e_1}=(a^{de_1})^{i_1}=(a^e)^{i_1}\equiv 1 \pmod p$$

であるから，e乗しなくても，e_1乗すれば1と合同になる．$(i, e)=1$のときはa^iはe乗しなければ1と合同にならない．なぜなら，

$$(a^i)^k\equiv 1 \pmod p$$

ならばikはeで割れる．$(i, e)=1$からkはeで割れる．よってa^iはe乗しなければ1と合同にならない．まとめると

(4) $$1,\ 2,\ 3,\ \cdots,\ p-1$$

の中にe乗すれば1と合同になるものは(2)で尽され，(2)の中でe乗してはじめて1と合同になるものは$(i, e)=1$のときのa^iで，その個数は$\varphi(e)$個である.

さて，$p-1$乗しなければ1と合同にならない数をpの**原始根**と呼ぶ．今までの議論から，もし原始根が1つでもあったならば，全部で$\varphi(p-1)$個あることがわかった．しかし，原始根が1つもないことは起るだろうか.

(4)の中でe乗してはじめて1と合同になる数があったとする．よってeは$p-1$の約数であり，e乗してはじめて1と合同となる数は(4)の中に$\varphi(e)$個ある．つまりeを$p-1$の約数とすると，e乗してはじめて1と合同となる数の個数は(4)の中に0個または$\varphi(e)$個である．また(4)のどの数も$p-1$の或る約数乗すれば1と合同となるのだから

(5) $$p-1\leqq\sum_{e|p-1}\varphi(e)$$

となる．右辺はeが$p-1$のすべての約数を動いたときの和である．ところが(5)の右辺は定理14により$p-1$に等しいので(5)は等式になる．つまり$p-1$のどの約数eを持ってきても，e乗してはじめて1と合同となる数が(4)の中に$\varphi(e)$個ある．特に$e=p-1$とすれば，

原始根が $\varphi(p-1)$ 個あることがわかった．まとめると次の定理を得る．

定理 16　素数 p と $p-1$ の約数 e に対し，e 乗してはじめて 1 と $\bmod p$ で合同になる数が $1, 2, \cdots, p-1$ の中に $\varphi(e)$ 個ある．特に $p-1$ 乗してはじめて 1 と合同になる数，つまり原始根は $\varphi(p-1)$ 個ある．——

例　$p=7$ のとき mod 7 で計算すると

$$3^1=3,\quad 3^2=9\equiv 2,\quad 3^3\equiv 2\cdot 3=6,\quad 3^4\equiv 6\cdot 3=18\equiv 4,$$
$$3^5\equiv 4\cdot 3=12\equiv 5,\quad 3^6\equiv 5\cdot 3=15\equiv 1$$

となり 3 は原始根である．また $(5,6)=1$ であるから $3^5\equiv 5$ も原始根である．この 2 つだけが原始根である．$3\equiv 10$ であるから，10 も原始根であるが，mod 7 で考えているとき，3 と 10 は同一視されている．——

r を素数 p の原始根とすると r の位数 $e=p-1$ であるから

$$(6)\qquad 1,\ r,\ r^2,\ \cdots,\ r^{p-2}$$

は $\bmod p$ で不合同である．また，これらは p で割れないから $\bmod p$ で考えれば $1, 2, \cdots, p-1$ のどれかである．しかも (6) は全部で $p-1$ 個あるから (6) は全体として $\bmod p$ で考えれば $1, 2, \cdots, p-1$ のすべてである．つまり p で割れない数は $\bmod p$ で考えれば原始根の巾乗として表わすことが出来る．

例　$p=31$ のとき，3 は原始根であり mod 31 で

$$1,\quad 3,\quad 3^2=9,\quad 3^3=27,\quad 3^4\equiv 19,\quad 3^5\equiv 26,\quad 3^6\equiv 16,$$
$$3^7\equiv 17,\quad 3^8\equiv 20,\quad 3^9\equiv 29,\quad 3^{10}\equiv 25,\quad 3^{11}\equiv 13,\quad 3^{12}\equiv 8,$$
$$3^{13}\equiv 24,\quad 3^{14}\equiv 10,\quad 3^{15}\equiv 30,\quad 3^{16}\equiv 28,\quad 3^{17}\equiv 22,\quad 3^{18}\equiv 4,$$
$$3^{19}\equiv 12,\quad 3^{20}\equiv 5,\quad 3^{21}\equiv 15,\quad 3^{22}\equiv 14,\quad 3^{23}\equiv 11,\quad 3^{24}\equiv 2,$$
$$3^{25}\equiv 6,\quad 3^{26}\equiv 18,\quad 3^{27}\equiv 23,\quad 3^{28}\equiv 7,\quad 3^{29}\equiv 21$$

となり，3 の巾より，1 から 30 までの数がすべて現われた．ただし

1は3^0と考えることにする. ——

例　$x^3\equiv 30 \pmod{31}$を解け.

解　もし解があったら, $x\equiv 0 \pmod{31}$ではあり得ない. よってxは原始根3の巾と表わせる. $x\equiv 3^n$とすれば前の例から$30\equiv 3^{15}$であるから

$$(7)\qquad 3^{3n} \equiv 3^{15} \pmod{31}$$

が得られる. フェルマーの定理から$3^{30}\equiv 1$であるから

$$(8)\qquad 3n \equiv 15 \pmod{30}$$

ならば(7)が成り立つ. 逆に(8)が成り立たなければ, $3n\equiv a \pmod{30}$, $0\leqq a\leqq 29$とすれば$a\neq 15$となるが, $3^0=1, 3^1=3, 3^2, \cdots, 3^{29}$はmod 31で不合同であるから, $3^{3n}\equiv 3^a$は3^{15}とmod 31で等しくない. よって(7)が成り立たない. つまり(7)が成り立てば, (8)が成り立つ. よって3次の合同式が1次の合同式(8)に帰着された. (8)の両辺および法を3で割り$n\equiv 5 \pmod{10}$が得られる. よって

$$n \equiv 5,\ 15,\ 25 \pmod{30}$$

となる. $x\equiv 3^n$であるから, 前の例から

$$x \equiv 26,\ 30,\ 6 \pmod{31}$$

が3個の解となる. ——

巻末に10000以下の奇素数の表と, その1つの原始根の表がある. 素数pの原始根は$\varphi(p-1)$個あるけれど, その中で, 素数であるもの, しかもその素数の中で最小な値を求めてみた. 多くの場合, 最小な原始根は素数であるが, そうでない場合の表もつけ加えた. 2つの表を比べれば, 最小な原始根が求まる. 表を見ると原始根が2であることが多い. 2を原始根に持つ素数は無限にあるだろうというのが**アルチンの予想**である.

§5 循環小数

ここに1つの真の既約分数$\dfrac{m}{n}$がある．つまり$0<m<n, (m, n)=1$となっていたとする．この分数を小数に展開したらどうなるだろうか．小数に展開する計算を考えてみると，mを10倍してnで割った商q_1が小数点以下1桁目であり，その余りを10倍しnで割った商が2桁目となる．つまり

$$10m = n\cdot q_1 + r_1$$
$$10r_1 = n\cdot q_2 + r_2$$

となったときのq_1, q_2が小数点以下1桁目，2桁目である．このとき

$$\begin{aligned}10^2 m &= 10nq_1 + 10r_1\\ &= n(10q_1) + nq_2 + r_2\\ &= n(10q_1 + q_2) + r_2\end{aligned}$$

となる．同様に計算を続けると，小数点以下1桁目からk桁目までの値$q_1q_2\cdots q_k = 10^{k-1}q_1 + 10^{k-2}q_2 + \cdots + q_k$とは$10^k\cdot m$を$n$で割った商であることがわかる．

少し計算してみると

$$\frac{3}{125} = 0.024$$
$$\begin{aligned}\frac{8}{35} &= 0.2285714285714\cdots\\ &= 0.2\dot{2}8571\dot{4}\end{aligned}$$

となり，割り切れるときと循環小数になる場合があるが，これら以外のことは起こらない．言いかえると循環しない無限小数になることはない．なぜなら，mをnで割っていくときはいつも余りrは$0\leqq r<n$であるが，何回も割り算を実行していくとき，$r=0$となれば割り切れた，ということになる．いつまで計算しても$r\neq 0$なら

ば $0<r<n$ となる r は $1, 2, \cdots, n-1$ のどれかであるから，多くとも n 回割り算を実行すれば，どこかに同じ余りが現われるはずである(部屋割り論法).

例

```
       0.2285714
   35)8.00000000
      7 0
      ------
      1 00*
         70
      -------
         300
         280
        -------
          200
          175
         -------
           250
           245
          -------
             50
             35
            -------
             150
             140
            -------
              100*
```

この計算では * をつけた 100 が同じ余りである. ——

余りが同じになればそこからの計算は前と同じであるから循環する.

さて m と n を与えた場合，循環するか否か，循環するときはどこからはじまり，循環節はどのくらい長くなるか，などについて話を進めよう.

まず $\frac{m}{n}$ が有限小数だったとする. 小数点以下 k 桁目までだとすると

$$\frac{m}{n}=\frac{q}{10^k}$$

という形となる. 分母を払うと

$$m\cdot 10^k = n\cdot q$$

となる. $(m, n)=1$ であるから 10^k は n で割れる. つまり n は素因

子として2と5以外はない．また$n=2^a\cdot 5^b$とし，aとbの大きい方をk_1とすると$k_1\leqq k$となる．

逆に$n=2^a\cdot 5^b$となっていたとする．aとbの大きい方をk_1とする．このとき10^{k_1}は$n=2^a\cdot 5^b$で割り切れるから$10^{k_1}\cdot m$もnで割り切れて，商をqとすると

$$\frac{m}{n}=\frac{1}{10^{k_1}}\frac{10^{k_1}\cdot m}{n}=\frac{q}{10^{k_1}}$$

となる．つまり$\dfrac{m}{n}$は小数点以下k_1桁目までの有限小数である．まとめると

定理 17　$\dfrac{m}{n}$が有限小数になる必要十分条件は，nの素因子が2と5以外にないことである．この場合，$n=2^a\cdot 5^b$, $\max\{a, b\}=k_1$とすると$\dfrac{m}{n}$は小数点以下k_1桁目でちょうど終る．——

次に循環する場合を考えよう．まず$\dfrac{m}{n}$が小数点以下$k+1$桁目から循環しはじめ，循環節の長さがe桁だったとする．つまり

$$\frac{m}{n}=\frac{q}{10^k}+\frac{1}{10^k}\left(\frac{c}{10^e}+\frac{c}{10^{2e}}+\frac{c}{10^{3e}}+\cdots\right)$$

となったとする．このとき等比数列の公式を用い

$$\begin{aligned}\frac{m}{n}&=\frac{q}{10^k}+\frac{1}{10^k}\frac{c}{(10^e-1)}\\&=\frac{q(10^e-1)+c}{10^k(10^e-1)}\\&=\frac{d}{10^k(10^e-1)}\qquad (d=q(10^e-1)+c)\end{aligned}$$

と変形出来る．分母を払うと

$$m\cdot 10^k\cdot(10^e-1)=n\cdot d$$

となる．$(m, n)=1$であるから$10^k(10^e-1)$はnで割り切れる．

$$n=2^a\cdot 5^b\cdot n_1,\qquad (10, n_1)=1$$

$$k_1 = \max\{a, b\}$$

とおくと $k \geqq k_1$ であり，10^e-1 が n_1 で割れる．つまり

$$10^e \equiv 1 \pmod{n_1}$$

となる．mod n_1 での 10 の位数を e_1 とすると，この式から e は e_1 の倍数でなければならない．k_1 および e_1 は n により定まる．このとき必ず $k_1 \leqq k$, $e_1 \leqq e$ となるわけである．

さて逆に $\dfrac{m}{n}$ を小数に展開すれば k_1+1 桁目から循環しはじめ，循環節の長さは e_1 と出来ることを示そう．

$$\frac{m}{n} = \frac{10^{k_1}\cdot m}{10^{k_1}\cdot n} = \frac{2^{k_1-a}\cdot 5^{k_1-b}\cdot m}{10^{k_1}\cdot n_1}$$

とおくと m と n は互いに素であり，n_1 は n の約数であるから m と n_1 も互いに素である．n_1 は 2 および 5 とも素であるから $m_1=2^{k_1-a}\cdot 5^{k_1-b}\cdot m$ と n_1 は互いに素である．よって m_1 を n_1 で割ると余りは 0 でなく

$$m_1 = n_1\cdot q+m_2, \qquad 0 < m_2 < n_1$$

とおくと

$$\frac{m}{n} = \frac{n_1\cdot q+m_2}{10^{k_1}\cdot n_1} = \frac{q}{10^{k_1}} + \frac{1}{10^{k_1}}\frac{m_2}{n_1}, \qquad (m_2, n_1) = 1$$

となる．mod n_1 での 10 の位数が e_1 であるから

$$m_2\cdot 10^{e_1} \equiv m_2 \pmod{n_1}$$

となる．つまり $\dfrac{m_2}{n_1}$ を小数に展開すると，小数点以下 e_1 桁まで計算したところで余りが最初の m_2 となる．よって e_1+1 桁目からは 1 桁目からと同じ数がならぶ．つまり $\dfrac{m_2}{n_1}$ は小数点第 1 位から循環し，循環節の長さは e_1 桁である．よって

$$\frac{m}{n} = \frac{q}{10^{k_1}} + \frac{1}{10^{k_1}}\left(\frac{c}{10^{e_1}} + \frac{c}{10^{2e_1}} + \frac{c}{10^{3e_1}} + \cdots\right)$$

となる．つまり $\dfrac{m}{n}$ は小数点以下 k_1+1 桁目から循環し，循環節の長

さは e_1 桁である．まとめると次の定理を得る．

定理 18 n が 2, 5 以外の素因子を持ち

$$n = 2^a \cdot 5^b \cdot n_1, \qquad (10, n_1) = 1$$

$$k_1 = \max\{a, b\}$$

$$e_1 = \bmod n_1 \text{ での } 10 \text{ の位数}$$

とおくと $\dfrac{m}{n}$ ははじめの k_1 桁は循環せず，k_1+1 桁目から循環しはじめ，循環節の長さは e_1 と出来る．循環しはじめる前の桁数および循環節の長さをこれ以上短くするまとめ方はない．——

例 $125=5^3$ であるから $\dfrac{1}{125}$ は小数点以下 3 桁目までの有限小数である．——

例 $35=5\cdot7$ であり $k_1=1$ となる．10 は mod 7 での原始根であるから 10 の位数は 6 となり，$\dfrac{8}{35}$ は小数点以下 2 桁目から循環しはじめ，循環節の長さは 6 桁である．——

§6 4n+1 となる素数

まず x を自然数とすると $(2x)^2+1$ はどのように素因子分解するか表を作ってみよう．

x	$(2x)^2+1$	x	$(2x)^2+1$	x	$(2x)^2+1$
1	5	11	$5\cdot97$	21	$5\cdot353$
2	17	12	577	22	$13\cdot149$
3	37	13	677	23	$29\cdot73$
4	$5\cdot13$	14	$5\cdot157$	24	$5\cdot461$
5	101	15	$17\cdot53$	25	$41\cdot61$
6	$5\cdot29$	16	$5^2\cdot41$	26	$5\cdot541$
7	197	17	$13\cdot89$	27	2917
8	257	18	1297	28	3137
9	$5^2\cdot13$	19	$5\cdot17^2$	29	$5\cdot673$
10	401	20	1601	30	$13\cdot277$

この表を見て気付くことは $p\equiv1 \pmod 4$ となる素因子しか現われ

ないことである．この事実は次のように証明される．

$(2x)^2+1$ は奇数であるから，素因子 p も奇数である．このとき

(1) $$(2x)^2 \equiv -1 \pmod{p}$$

であるから自乗して

(2) $$(2x)^4 \equiv 1 \pmod{p}$$

となる．よって $2x$ の位数 e は 4 の約数であるが，4 の約数は 1, 2, 4 の 3 つである．もし $e=1$ ならば $2x\equiv1$ となり $(2x)^2\equiv1$ となり (1) から $1\equiv-1 \pmod{p}$ となる．ところが p は奇数であるから矛盾である．よって $e\neq1$ である．同様に $e\neq2$ であるから $e=4$ となる．さて位数は $\varphi(p)=p-1$ の約数であるから $p-1$ は 4 で割れる．つまり $(2x)^2+1$ の素因子はすべて $p\equiv1 \pmod{4}$ となることがわかった．

逆に $p\equiv1 \pmod{4}$ となる素数は $1<2x\leqq p-1$ なる適当な x に対して $(2x)^2+1$ の素因子となることが次のように示される．

$p\equiv1 \pmod{4}$ のとき 4 は $p-1$ の約数である．よって 4 乗してはじめて 1 と合同となる数が $1, 2, \cdots, p-1$ の中に $\varphi(4)=2$ 個ある．その 1 つを y とすれば $y^4\equiv1 \pmod{p}$ となる．y は 4 乗しなければ 1 と合同にならないから $y^2\not\equiv1 \pmod{p}$ である．さて $y^4-1=(y^2-1)(y^2+1)$ は p で割れるから y^2-1 または y^2+1 が p で割れる．しかし $y^2\not\equiv1 \pmod{p}$ であるから y^2+1 が p で割れることが得られた．y が偶数ならば $y=2x$ とおき，y が奇数ならば $p-y=2x$ とおけば $1<2x\leqq p-1$ となり

$$(2x)^2+1 = y^2+1 \equiv 0 \pmod{p}$$

または

$$= (p-y)^2+1 \equiv y^2+1 \equiv 0 \pmod{p}$$

から p は $(2x)^2+1$ の素因子となる．

次に $p\equiv1 \pmod{4}$ となる素数は無限にあることを証明しよう．背理法を用い，もし $p\equiv1 \pmod{4}$ となる素数が有限個しかないと仮

定し，それらを $5, 13, 17, \cdots, p_n$ としよう．

$$a = (2\cdot 5\cdot 13\cdot 17\cdot\cdots\cdot p_n)^2+1$$

とおくと，a を割る素数 p は $p\equiv 1 \pmod 4$ しかない．しかし a を 5, 13, 17, $\cdots, p_n$ のどれで割っても 1 余るから矛盾である．よって $p\equiv 1 \pmod 4$ となる素数が無限にあることが示された．

130 ページの表を見ると $x=1, 2, 3, 5, 7, \cdots$ のとき $(2x)^2+1$ が素数になっている．$(2x)^2+1$ という形をした素数は無限にあるだろうか．これは未解決な難問である．ディリクレにより，$(a, b)=1$ ならば $ax+b$ という 1 次式の形をした素数は無限にあることが証明されているが，2 次式以上になると，何も証明されていないわけである．

次に $p\equiv 1 \pmod 4$ となる素数は 2 つの平方数の和になることを示そう．

例

$$\begin{aligned} 5 &= 2^2+1^2, & 13 &= 3^2+2^2, \\ 17 &= 4^2+1^2, & 29 &= 5^2+2^2, \\ 37 &= 6^2+1^2, & 41 &= 5^2+4^2, \\ 53 &= 7^2+2^2, & 61 &= 6^2+5^2, \\ 73 &= 8^2+3^2, & 89 &= 8^2+5^2, \\ 97 &= 9^2+4^2, & 101 &= 10^2+1^2. \text{ ——} \end{aligned}$$

まず $(2x)^2+1\equiv 0 \pmod p$ となる x が存在するので，$2x=t$ とおけば

(3)
$$t^2 \equiv -1 \pmod p$$

となる．以後 t を固定する．自然数 e を

(4)
$$(e-1)^2 < p < e^2$$

となるように定める．次に x と y を 0 から $e-1$ まで別々に動かして $x-yt$ という値を考える．x と y は e 個の値を動くので，全部で e^2 個の値が出来る．(4) から e^2 は p より大きいので，部屋割り論法により $\mathrm{mod}\, p$ で考えると同じ類に入っているものがある．すなわち

$$x_1-y_1t \equiv x_2-y_2t \pmod p$$

$$0 \leqq x_1, x_2, y_1, y_2 < e$$

となる組合せが存在する．このとき

$$(5) \qquad x_1-x_2 \equiv (y_1-y_2)t \pmod p$$

$$-e < x_1-x_2 < e, \qquad -e < y_1-y_2 < e$$

であるから(4)から

$$(6) \qquad 2p > 2(e-1)^2 \geqq (x_1-x_2)^2+(y_1-y_2)^2 > 0$$

となり(5)と(3)から

$$\begin{aligned}(x_1-x_2)^2+(y_1-y_2)^2 &\equiv (y_1-y_2)^2t^2+(y_1-y_2)^2 \pmod p\\ &\equiv -(y_1-y_2)^2+(y_1-y_2)^2 \pmod p\\ &= 0\end{aligned}$$

となる．よって $(x_1-x_2)^2+(y_1-y_2)^2$ は p で割り切れ，しかも(6)から $0<(x_1-x_2)^2+(y_1-y_2)^2<2p$ であるから

$$p = (x_1-x_2)^2+(y_1-y_2)^2$$

となる．これで $p\equiv 1 \pmod 4$ ならば，2つの平方数の和になることが示された．よって次の定理を得る．

定理 19　$p\equiv 1 \pmod 4$ となる素数は無限にある．また，これらの素数はどれも2つの平方数の和として表わすことが出来る．——

後　編

第7章　相　互　律

1次合同式と異なり，2次合同式では解を求める良い方法がない．しかし解があるか否かの判定だけは相互律を用いると非常に能率的に計算出来る．この章では，相互律を証明し，2次合同式に解があるか否かの能率的な判定法を示そう．また相互律そのものは，非常に美しい定理であるから，ゆっくり味わってもらいたい．しかし相互律の本当の意味は，より進んだ整数論を学んだときに，はっきりしてくる．このような意味で，相互律は初等整数論の中における一番味わい深い定理といえよう．

§1　2次合同式

1次合同式を具体的に与えたとき，その式に解が存在するか否か，存在するときはいかに能率的に解を求めるか，ということはユークリッドの互除法を用いて完全にわかっている．2次合同式の場合はどうだろうか．一般の自然数 m を法とする合同式を考えるべきだけれど，少し煩わしいので，本質的な部分，すなわち法が素数の場合のみを考えよう．

まず，法が素数2の場合を考えよう．そのとき2次合同式は

$$x^2 \equiv 0 \pmod 2$$

$$x^2+1 \equiv 0 \pmod 2$$

$$x^2+x \equiv 0 \pmod 2$$

$$x^2+x+1 \equiv 0 \pmod 2$$

の4つである．1番目は $x\equiv 0$ が解である．2番目は $x\equiv 1$ が解である．3番目は $x\equiv 0, x\equiv 1$ の両方が解である．4番目は解がない．こ

のように法が 2 のときは完全にわかるので，以後 p を奇素数として，p を法とする合同式を考えよう．

奇素数 p を法とする一般の 2 次合同式は

$$(1)\qquad ax^2+bx+c \equiv 0 \pmod p, \qquad (a,p)=1$$

と書ける．$(a,p)=1$ であるから $ad\equiv 1 \pmod p$ となる d が定まる．(1)の両辺に d を掛けると

$$(2)\qquad x^2+bdx+cd \equiv 0 \pmod p$$

となる．$(2,p)=1$ であるから $2e\equiv bd \pmod p$ となる e が定まる．$f=cd$ とおけば(2)は

$$x^2+2ex+f \equiv 0 \pmod p$$

となる．2 次方程式を解くときと同じように平方を完成させると

$$(x+e)^2+f-e^2 \equiv 0 \pmod p$$

となる．$y=x+e, g=e^2-f$ とおけば

$$(3)\qquad y^2 \equiv g \pmod p$$

となる．よって(1)が解けるか否かは(3)が解けるか否かと同値になる．

例　$2x^2+3x+1\equiv 0 \pmod 7$ を解け．

解　$2\cdot 4=8\equiv 1 \pmod 7$ であるから，両辺を 4 倍すると x^2 の係数は 1 と合同になり，

$$x^2+12x+4 \equiv 0 \pmod 7$$

となる．平方を完成すると

$$\begin{aligned}(x+6)^2 &\equiv 36-4 \pmod 7\\ &\equiv 4 \pmod 7\end{aligned}$$

となる．$x+6=y$ とおくと $y^2\equiv 4 \pmod 7$ となり $(y-2)(y+2)$ が 7 で割れる．よって $y-2$ または $y+2$ が 7 で割れ，$y\equiv 2$ または $y\equiv -2$ となる．$x=y-6$ であるから $x\equiv -4\equiv 3$ または $x\equiv -8\equiv 6$ が答となる．——

よって，大切なことは(3)が解けるか否か，解けるならばいかに解を求めるか，ということになる．後に述べる相互律を使うと，(3)が解けるか否かだけは，ユークリッドの互除法と同じように能率よく判定出来る．

例 $x^2\equiv-1 \pmod p$ が解を持つ必要十分条件は $p\equiv1 \pmod 4$ となることを示せ．

解 原始根を使うと次のように説明出来る．まず，与えられた2次合同式に解があるならば，その解 x の位数 e を求めると $x^2\equiv-1$, $x^4\equiv1$ から $e=4$ となる．位数は $\varphi(p)=p-1$ の約数だから $p\equiv1$ $\pmod 4$ が得られた．

逆に $p\equiv1 \pmod 4$ のとき，p の原始根を r とすれば，r は $p-1$ 乗してはじめて1と合同になる．$x=r^{(p-1)/4}$ とおけば $x^4=r^{p-1}\equiv1$ となる．よって $x^4-1=(x^2-1)(x^2+1)$ が p で割れるので，x^2-1 または x^2+1 が p で割れる．もし x^2-1 が p で割れると

$$r^{(p-1)/2}=x^2\equiv1 \pmod p$$

となり，r が原始根であることに反する．原始根は $p-1$ 乗より小さな巾乗では1と合同とならないからである．よって x^2+1 が p で割れる．つまり解が得られた．——

例 $x^2\equiv-1 \pmod{13}$ を解け．

解 $13\equiv1 \pmod 4$ であるから解はある．mod 13で計算すると，$a^2\equiv(13-a)^2$ であるから a を1より大きくしていくと

$$1^2\equiv12^2\equiv1$$
$$2^2\equiv11^2\equiv4$$
$$3^2\equiv10^2\equiv9$$
$$4^2\equiv9^2\equiv16\equiv3$$
$$5^2\equiv8^2\equiv25\equiv-1$$

となり $x\equiv5, 8$ が解となる．2次合同式は2個より多く解を持たな

いから，この2つが解のすべてである．——

例 $x^2 \equiv -1 \pmod{401}$ を解け．

解 $401 \equiv 1 \pmod 4$ であるから解はある．巻末の最小素数原始根の表を見ると，3が原始根であるから $3^{(401-1)/4}=3^{100}$ が解である．100を2進法で表わすと1100100であるから mod 401 で計算すると

$$
\begin{aligned}
3^3 &= 27 \\
3^6 &= 27^2 \equiv 328 \\
3^{12} &\equiv 328^2 \equiv 116 \\
3^{25} &= (3^{12})^2 \cdot 3 \equiv 116^2 \cdot 3 \equiv 268 \\
3^{50} &\equiv 268^2 \equiv 45 \\
3^{100} &\equiv 45^2 \equiv 20
\end{aligned}
$$

と計算され，20が1つの解になる．$20^2=400\equiv -1$ であるから確かに解である．もう1つの解は $401-20=381$ である．——

例 素数 p の原始根を r とし，$a\equiv r^m \pmod p$ のとき $x^2\equiv a \pmod p$ が解を持つ必要十分条件は，m が偶数であることを示せ．

解 r の位数は $p-1$ であるから

$$r^m \equiv r^n \pmod p \qquad (m<n)$$

のとき，両辺を r^m で割り $r^{n-m}\equiv 1$ が得られ，$n-m$ が $p-1$ で割れることが得られる．$p-1$ は偶数であるから（p は奇素数だと制限してある），n が偶数ならば m も偶数となる．さて解 x があるとき，$a\not\equiv 0$ であるから $x\not\equiv 0$ である．よって $x\equiv r^k$ と原始根の巾乗で表わせる．このとき $r^{2k}\equiv x^2\equiv a\equiv r^m$ であるから m は偶数でなければいけない．逆に m が偶数ならば $m=2k$ とおき $x=r^k$ とおけば $x^2=r^{2k}=r^m\equiv a$ となる．——

例 $(a,p)=1$ のとき $x^2\equiv a \pmod p$ が解を持つ必要十分条件は $a^{(p-1)/2}\equiv 1 \pmod p$ であることを示せ．

解 p の原始根を r とし，$a=r^m$ とする．もし m が偶数で $m=2k$

となったならば

$$\begin{aligned} a^{(p-1)/2} &\equiv r^{2k\cdot(p-1)/2} \pmod p \\ &= (r^{p-1})^k \\ &\equiv 1 \pmod p \end{aligned}$$

となる．逆に $a^{(p-1)/2}\equiv 1$ ならば

$$\begin{aligned} 1 &\equiv a^{(p-1)/2} \pmod p \\ &\equiv r^{m\cdot(p-1)/2} \pmod p \end{aligned}$$

となり，r が原始根であることから $m\cdot(p-1)/2$ が $p-1$ で割れる．つまり $m/2$ は整数となり，m は偶数となる．——

例　$x^2\equiv 2 \pmod{101}$ は解があるか．

解　$(101-1)/2=50$ を2進法で表わすと110010である．よって 2^{50} を mod 101 で計算すると

$$\begin{aligned} 2^3 &= 8 \\ 2^6 &= 8^2 = 64 \\ 2^{12} &= 64^2 \equiv 56 \\ 2^{25} &= (2^{12})^2\cdot 2 \equiv 56^2\cdot 2 \equiv 10 \\ 2^{50} &\equiv 10^2 = 100 \equiv -1. \end{aligned}$$

よって解は存在しない．——

§2　ルジャンドル記号

奇素数 p に対し

(1)　$$x^2 \equiv a \pmod p$$

に解があるとき，a を**平方剰余**という．或る数を平方し，p で割った余りが a となるからである．(1)に解がないとき，a を**平方非剰余**という．a が p で割り切れれば(1)は $x\equiv 0$ という自明な解を持つ．以後 a は p と素としよう．つまり a は p で割り切れないとしよう．さて

$$\left(\frac{a}{p}\right)=\begin{cases} 1, & a=\text{平方剰余の場合} \\ -1, & a=\text{平方非剰余の場合} \end{cases}$$

と定義する．この記号を**ルジャンドル記号**という．

例　mod 5 で考えると

$$1^2=1, \quad 2^2=4, \quad 3^2\equiv 4, \quad 4^2\equiv 1$$

であるから，

$$\left(\frac{1}{5}\right)=\left(\frac{4}{5}\right)=1, \quad \left(\frac{2}{5}\right)=\left(\frac{3}{5}\right)=-1$$

となる．——

さて，次に a がどのようなとき平方剰余となるかを考えよう．

$a=1$ ならば $1^2\equiv 1 \pmod p$ であるから

$$\left(\frac{1}{p}\right)=1$$

となる．$a\equiv b \pmod p$ ならば $x^2\equiv a$ が解を持つことと，$x^2\equiv b$ が解を持つこととは同じことであるから

$$a\equiv b \pmod p \Longrightarrow \left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$$

となる．次に原始根を使わずに

$$\left(\frac{a}{p}\right)\equiv a^{(p-1)/2} \pmod p \tag{2}$$

を示そう．

$1\leqq x\leqq p-1$ となる x に対し $(x,p)=1$ であるから

$$x\cdot y\equiv a \pmod p \qquad (1\leqq y\leqq p-1)$$

となる y はただ1つ定まる．この y を x の配偶と呼ぼう．すると自分自身が配偶となる可能性は，a が平方剰余のときにかぎる．a が平方剰余のとき

$$x^2\equiv a \pmod p \qquad (1\leqq x\leqq p-1)$$

の1つの解を x_0 とすれば，

$$(p-x_0)^2 = p^2-2px_0+x_0{}^2$$
$$\equiv x_0{}^2 \pmod p$$
$$\equiv a \pmod p$$

となり $p-x_0$ も解となり $1 \leqq p-x_0 \leqq p-1$ となる．しかも $x_0=p-x_0$ となることはない．p が奇数だからである．よって1から $p-1$ までの中で x_0 と $p-x_0$ の2つだけが自分自身を配偶に持ち，他は自分と異なる配偶を持つ．1から $p-1$ までを並べかえて

$$x_0,\ p-x_0,\ x_1,\ x_2,\ \cdots,\ x_{(p-3)/2},\ y_1,\ y_2,\ \cdots,\ y_{(p-3)/2}$$

としよう．x_i の配偶を y_i とするのである．よって

$$(p-1)! = x_0(p-x_0)(x_1\cdot y_1)(x_2\cdot y_2)\cdots(x_{(p-3)/2}\cdot y_{(p-3)/2})$$
$$\equiv x_0(-x_0)\cdot a\cdot a\cdot\cdots\cdot a \pmod p$$
$$\equiv -a^{(p-1)/2} \pmod p$$

となる．特に $a=1$ のときは，a は平方剰余であるから $(p-1)!\equiv -1$ となる（ウィルソンの定理）．この式をふたたび上式に代入すると

(3) $$a = \text{平方剰余} \Longrightarrow a^{(p-1)/2} \equiv 1 \pmod p$$

が得られた．a が平方非剰余のときは，自分自身を配偶に持つ数はないので1から $p-1$ までの数を並べかえ

$$x_1,\ x_2,\ \cdots,\ x_{(p-1)/2},\ y_1,\ y_2,\ \cdots,\ y_{(p-1)/2}$$

とおく．y_i は x_i の配偶である．このとき

$$(p-1)! = (x_1\cdot y_1)(x_2\cdot y_2)\cdot\cdots\cdot(x_{(p-1)/2}\cdot y_{(p-1)/2})$$
$$\equiv a\cdot a\cdot\cdots\cdot a \pmod p$$
$$= a^{(p-1)/2} \pmod p$$

となる．よって，ウィルソンの定理を使い

(4) $$a = \text{平方非剰余} \Longrightarrow a^{(p-1)/2} \equiv -1 \pmod p$$

が得られた．(3)と(4)をまとめると，ルジャンドル記号の定義から(2)が得られる．(2)を**オイラーの規準**という．

$a=-1$ の場合を考えよう．$(p-1)/2$ が偶数になるのは $p\equiv 1$ (mod

4) の場合だから，このとき(2)から

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod p$$
$$= 1$$

となる．左辺は 1 または -1 だが，p が奇素数なので $-1 \not\equiv 1$ である．よって

$$p \equiv 1 \pmod 4 \Longrightarrow \left(\frac{-1}{p}\right) = 1$$

が得られた．同様にして

$$p \equiv 3 \pmod 4 \Longrightarrow \left(\frac{-1}{p}\right) = -1$$

となる．まとめると

$$(5) \qquad \left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 4 \text{ の場合} \\ -1, & p \equiv 3 \pmod 4 \text{ の場合} \end{cases}$$

となる．次に(2)を使うと

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \pmod p$$
$$= a^{(p-1)/2} \cdot b^{(p-1)/2}$$
$$\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$$

となる．よって

$$\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$$

だけれど，左辺，右辺とも 1 または -1 である．ところが $1 \not\equiv -1$ であるから，この合同式は等式となる．つまり

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

が得られた．この式から一般に $\left(\frac{a}{p}\right)$ を計算するには a を素因子分

解して$\left(\dfrac{2}{p}\right)$および$q$を奇素数としたときの$\left(\dfrac{q}{p}\right)$が計算出来ればよい．ところが次節に証明するように

$$(6)\qquad \left(\frac{2}{p}\right)=\begin{cases} 1, & p\equiv 1 \text{ または } 7 \pmod 8 \text{ の場合} \\ -1, & p\equiv 3 \text{ または } 5 \pmod 8 \text{ の場合}\end{cases}$$

$$(7)\qquad \left(\frac{q}{p}\right)=\begin{cases} \left(\dfrac{p}{q}\right), & p\equiv 1 \text{ または } q\equiv 1 \pmod 4 \text{ の場合} \\ -\left(\dfrac{p}{q}\right), & p\equiv q\equiv 3 \pmod 4 \text{ の場合}\end{cases}$$

が成り立つ．(7)を**平方剰余の相互法則**(または相互律)といい，(5)をその**第1補充法則**，(6)を**第2補充法則**という．これらの性質を使えばルジャンドル記号は容易に計算出来る．

例　$\left(\dfrac{30}{97}\right)=\left(\dfrac{2}{97}\right)\left(\dfrac{3}{97}\right)\left(\dfrac{5}{97}\right).$

$97\equiv 1 \pmod 8$ だから(6)から

$$=\left(\frac{3}{97}\right)\left(\frac{5}{97}\right)$$

$97\equiv 1 \pmod 4$ だから(7)から

$$=\left(\frac{97}{3}\right)\left(\frac{97}{5}\right)$$

$97\equiv 1 \pmod 3$,　$97\equiv 2 \pmod 5$ だから

$$=\left(\frac{1}{3}\right)\left(\frac{2}{5}\right)$$

$$=\left(\frac{2}{5}\right)$$

$5\equiv 5 \pmod 8$ だから(6)から

$$=-1$$

となる．よって

$$x^2\equiv 30 \pmod{97}$$

は整数解がない．——

§3　相互律の証明

相互律は初等整数論における一番味わい深い定理である．この定理はオイラーにより予想され，ガウス(1777–1855)によってはじめて証明された．ガウスが24歳のときにこの証明は発表されたが，このとき整数論がパズル的な世界から，真の学問の世界へと進んだと言ってよい．定理の意味を考えると，p と q が奇素数のとき

$$x^2 \equiv q \pmod p$$

が解を持つか否かが

$$x^2 \equiv p \pmod q$$

が解を持つか否かに帰着されるのだから，不思議な定理である．証明は少し長くなるが，まずはガウスの補題からはじめよう．

一般に a を $b(>0)$ で割った余り r は $0 \leqq r < b$ である．もし $b/2 < r < b$ ならば，$-b/2 < r-b < 0$ であるから

$$a = bq' + r' \qquad (-b/2 < r' \leqq b/2)$$

となる r' が定まる．この r' を**絶対値最小な余り**という．

さてaを奇素数 p と素な数とし，

(1)
$$a,\ 2a,\ \cdots,\ \frac{p-1}{2}a$$

を p で割った絶対値最小な余りのうち，負なものの個数を n とする．このとき

(2)
$$\left(\frac{a}{p}\right) = (-1)^n$$

が成り立つ(**ガウスの補題**)．

なぜならば，負になる余りを $r_1, r_2, \cdots, r_n$ とし，正になる余りを $r_{n+1}, \cdots, r_{(p-1)/2}$ としたとき

(3) $$-r_1, -r_2, \cdots, -r_n, r_{n+1}, \cdots, r_{(p-1)/2}$$

という$(p-1)/2$個の数は$1, 2, \cdots, (p-1)/2$のどれかであるが，(3)の中に等しいものはない．それは

$$-\frac{p-1}{2}, \cdots, -2, -1, 1, 2, \cdots, \frac{p-1}{2}$$

は$\mathrm{mod}\, p$で不合同だからaを掛けた，

(4) $$-\frac{p-1}{2}a, \cdots, -2a, -a, a, 2a, \cdots, \frac{p-1}{2}a$$

も$\mathrm{mod}\, p$で不合同である．(3)の数は(4)の中の$\dfrac{p-1}{2}$個の値をpで割った余りであるから，(3)の数は$\mathrm{mod}\, p$で不合同，よって等しいものはない．(3)の数は$1, 2, \cdots, (p-1)/2$のどれかであり，$(p-1)/2$個あり，しかも等しいものはない．つまり$1, 2, \cdots, (p-1)/2$を並べかえたものである．しかも(1)をpで割った絶対値最小の余りが$r_1, \cdots, r_{(p-1)/2}$である．よって

$$a\cdot 2a\cdot\cdots\cdot\frac{p-1}{2}a \equiv r_1\cdot r_2\cdot\cdots\cdot r_{(p-1)/2} \pmod p$$

$$= (-1)^n(-r_1)(-r_2)\cdots(-r_n)\cdot r_{n+1}\cdot\cdots\cdot r_{(p-1)/2}$$

$$= (-1)^n\cdot 1\cdot 2\cdot\cdots\cdot\frac{p-1}{2}.$$

よって両辺を$1\cdot 2\cdot\cdots\cdot(p-1)/2$で割り

$$a^{(p-1)/2} \equiv (-1)^n \pmod p$$

が得られた．オイラーの規準を用いると

$$\left(\frac{a}{p}\right) \equiv (-1)^n \pmod p$$

となるが，両辺は1または-1であるから(2)が得られた．

$a=-1$の場合を考えよう．このとき

$$-1,\ -2,\ \cdots,\ -\frac{p-1}{2}$$

の中で p で割った絶対値最小の余りが負になるものは全部である．よって $n=(p-1)/2$ となり

$$\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}$$

つまり第1補充法則がふたたび証明された．

次に $a=2$ としてみよう．すると

$$2,\ 4,\ 6,\ \cdots,\ p-1$$

の中で p で割ったとき，絶対値最小の余りが負になる数は，$p/2<x<p$ となる偶数である．$p/2$ 以上の偶数の個数は

（イ） $p=8m+1$ のとき，$(p-1)/2=4m=$偶数 だから

$$4m+2,\ 4m+4,\ \cdots,\ 4m+2\cdot(2m)$$

の $2m$ 個である．

（ロ） $p=8m+3$ のとき，$(p-1)/2=4m+1=$奇数 だから

$$4m+2,\ 4m+4,\ \cdots,\ 4m+2\cdot(2m+1)$$

の $2m+1$ 個である．

（ハ） $p=8m+5$ のとき，$(p-1)/2=4m+2=$偶数 だから

$$4m+4,\ 4m+6,\ \cdots,\ 4m+2\cdot(2m+2)$$

の $2m+1$ 個である．

（ニ） $p=8m+7$ のとき，$(p-1)/2=4m+3=$奇数 だから

$$4m+4,\ 4m+6,\ \cdots,\ 4m+2\cdot(2m+3)$$

の $2m+2$ 個である．

結局

$$\left(\frac{2}{p}\right)=(-1)^n=\begin{cases}\ \ 1, & p\equiv 1 \text{ または } p\equiv 7 \pmod 8 \text{ の場合}\\ -1, & p\equiv 3 \text{ または } p\equiv 5 \pmod 8 \text{ の場合}\end{cases}$$

となり，第2補充法則が証明された．言いかえると

$$x^2\equiv 2 \pmod p$$

が解を持つための必要十分条件は

$$p \equiv 1 \quad \text{または} \quad p \equiv 7 \pmod 8$$

である．

次に相互律の証明であるが，日本の数学を世界的に高めた高木貞治博士が工夫した証明を紹介しよう．

まず図7-1のような平面図を考えよう．そして $y=\dfrac{q}{p}x$ という直線を引く．このとき

(5) $$q,\ 2q,\ \cdots,\ \frac{p-1}{2}q$$

を p で割ったとき，絶対値最小の余りが負になるとは，たとえば i 番目の iq に対して考えると

$$iq = p\cdot t + r, \qquad -\frac{p}{2} < r < 0$$

となることで，両辺を p で割ると，

$$i\frac{q}{p} = t + \frac{r}{p}, \qquad -\frac{1}{2} < \frac{r}{p} < 0$$

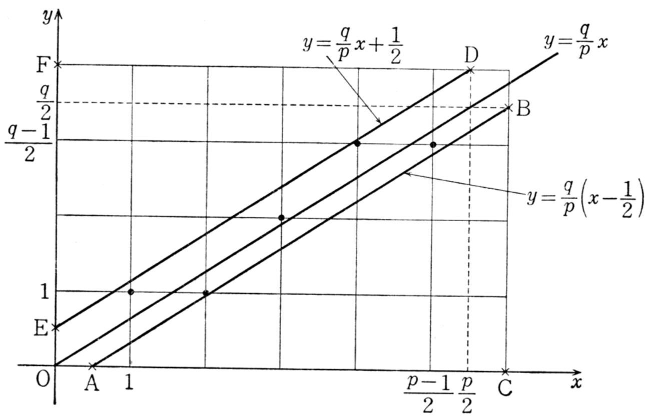


図 7-1

となることで，これは $y=\dfrac{q}{p}x$ において，$x=i$ のときの値が整数 t より少し下にあることを意味する．正確に書くと

$$i\frac{q}{p}<t<i\frac{q}{p}+\frac{1}{2}$$

となる整数 t があることを意味する．点 (i, t) は x 座標も，y 座標も整数である．このような点を**格子点**と呼ぶ．すると(5)を p で割ったとき，絶対値最小の余りが負になる数の個数は

$$y=\frac{q}{p}x$$

$$y=\frac{q}{p}x+\frac{1}{2} \qquad \left(1\leqq x\leqq \frac{p-1}{2}\right)$$

となる直線にかこまれた平行四辺形の周および内部にある格子点の個数(n 個としよう)と等しい．同様に

$$p,\ 2p,\ \cdots,\ \frac{q-1}{2}p$$

を q で割ったとき，絶対値最小の余りが負になる数の個数は

$$x=\frac{p}{q}y \qquad \left(\text{つまり}\ y=\frac{q}{p}x\right)$$

$$x=\frac{p}{q}y+\frac{1}{2} \qquad \left(\text{つまり}\ y=\frac{q}{p}\left(x-\frac{1}{2}\right)\right)$$

$$1\leqq y\leqq \frac{q-1}{2}$$

にかこまれた平行四辺形の周および内部にある格子点の個数(m 個としよう)と等しい．

三角形 ABC と三角形 DEF の内部にある格子点の個数は等しいし(k 個としよう)，全部合わせると長方形の内部にある格子点の個数になるので

$$n+m+2k=\frac{p-1}{2}\cdot\frac{q-1}{2}$$

となる．よってガウスの補題から

$$\begin{aligned}\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)&=(-1)^n(-1)^m\\&=(-1)^{n+m+2k}\\&=(-1)^{(p-1)/2\cdot(q-1)/2}\end{aligned}$$

となる．$\dfrac{p-1}{2}\cdot\dfrac{q-1}{2}$ が奇数になるのは $\dfrac{p-1}{2}=$奇数，$\dfrac{q-1}{2}=$奇数のときである．つまり $p\equiv3\ (\mathrm{mod}\ 4)$，$q\equiv3\ (\mathrm{mod}\ 4)$ の場合である．よって

$$\left(\frac{q}{p}\right)=\begin{cases}\left(\dfrac{p}{q}\right), & p\equiv1\ \text{または}\ q\equiv1\ (\mathrm{mod}\ 4)\ \text{の場合}\\ -\left(\dfrac{p}{q}\right), & p\equiv q\equiv3\ (\mathrm{mod}\ 4)\ \text{の場合}\end{cases}$$

となり相互律の証明が終った．まとめると

定理 20（相互律）　奇素数 p, q に対して

$$\left(\frac{-1}{p}\right)=\begin{cases}1, & p\equiv1\ (\mathrm{mod}\ 4)\ \text{の場合}\\ -1, & p\equiv3\ (\mathrm{mod}\ 4)\ \text{の場合}\end{cases}$$

$$\left(\frac{2}{p}\right)=\begin{cases}1, & p\equiv\pm1\ (\mathrm{mod}\ 8)\ \text{の場合}\\ -1, & p\equiv\pm3\ (\mathrm{mod}\ 8)\ \text{の場合}\end{cases}$$

$$\left(\frac{q}{p}\right)=\begin{cases}\left(\dfrac{p}{q}\right), & p\equiv1\ \text{または}\ q\equiv1\ (\mathrm{mod}\ 4)\ \text{の場合}\\ -\left(\dfrac{p}{q}\right), & p\equiv q\equiv3\ (\mathrm{mod}\ 4)\ \text{の場合}\end{cases}$$

となる．——

例　図 7-1 は $p=11$，$q=7$ の場合である．このとき

$$n=3,\ \ m=2,\ \ k=5$$

となり

$$\frac{p-1}{2}\cdot\frac{q-1}{2}=3+2+2\times 5$$

$$=15$$

$$=\text{奇数}$$

となっている．よって

$$\left(\frac{7}{11}\right)=-\left(\frac{11}{7}\right)$$

である．——

例 $p\equiv 1$ または $p\equiv 3 \pmod 8$ のときにかぎり

$$x^2\equiv -2 \pmod p$$

は解があることを示せ．

解 $p\equiv 1 \pmod 8$ のときは $p\equiv 1 \pmod 4$ であるから

$$\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\cdot\left(\frac{2}{p}\right)=1\cdot 1=1.$$

$p\equiv 3 \pmod 8$ のときは $p\equiv 3 \pmod 4$ であるから

$$\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)=(-1)\cdot(-1)=1.$$

$p\equiv 5 \pmod 8$ のときは $p\equiv 1 \pmod 4$ であるから

$$\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)=1\cdot(-1)=-1.$$

$p\equiv 7 \pmod 8$ のときは $p\equiv 3 \pmod 4$ であるから

$$\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)=(-1)\cdot 1=-1.$$

以上から $p\equiv 1$ または $p\equiv 3 \pmod 8$ のときのみ $\left(\frac{-2}{p}\right)=1$ となる．

——

例 $\left(\frac{181}{1489}\right)=\left(\frac{1489}{181}\right) \qquad \because\ 181\equiv 1 \pmod 4$

$$=\left(\frac{41}{181}\right) \qquad \because\ 1489\equiv 41 \pmod{181}$$

$$= \left(\frac{181}{41}\right) \qquad \because \quad 181 \equiv 1 \pmod 4$$

$$= \left(\frac{17}{41}\right) \qquad \because \quad 181 \equiv 17 \pmod{41}$$

$$= \left(\frac{41}{17}\right) \qquad \because \quad 17 \equiv 1 \pmod 4$$

$$= \left(\frac{7}{17}\right) \qquad \because \quad 41 \equiv 7 \pmod{17}$$

$$= \left(\frac{17}{7}\right) \qquad \because \quad 17 \equiv 1 \pmod 4$$

$$= \left(\frac{3}{7}\right) \qquad \because \quad 17 \equiv 3 \pmod 7$$

$$= -\left(\frac{7}{3}\right) \qquad \because \quad 7 \equiv 3 \pmod 4$$

$$= -\left(\frac{1}{3}\right) \qquad \because \quad 7 \equiv 1 \pmod 3$$

$$= -1.$$

この例の場合は，現われる数はすべて奇素数なので，このように互除法と同じような計算が出来る．——

§4 ヤコビの記号

ルジャンドル記号は素因子分解とユークリッドの互除法のような割り算をくり返せば計算出来るか，じつは素因子分解せずとも計算出来る．

まず m を奇数である自然数としよう．m を素因子分解して $m=p_1p_2\cdots p_r$ のとき，$(m, n)=1$ となる n に対して

$$\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right)\left(\frac{n}{p_2}\right)\cdots\left(\frac{n}{p_r}\right)$$

と定義する．これを**ヤコビの記号**という．

$\left(\dfrac{1}{p_i}\right)=1$ であるから

$$\left(\frac{1}{m}\right)=\left(\frac{1}{p_1}\right)\left(\frac{1}{p_2}\right)\cdots\left(\frac{1}{p_r}\right)=1$$

となる.

また $n\equiv n' \pmod{m}$ ならば p_i が m の約数なので $n\equiv n' \pmod{p_i}$ となる．よって

$$\begin{aligned}\left(\frac{n'}{m}\right)&=\left(\frac{n'}{p_1}\right)\left(\frac{n'}{p_2}\right)\cdots\left(\frac{n'}{p_r}\right)\\&=\left(\frac{n}{p_1}\right)\left(\frac{n}{p_2}\right)\cdots\left(\frac{n}{p_r}\right)\\&=\left(\frac{n}{m}\right)\end{aligned}$$

が得られる.

次に第1補充法則であるが，$p_1, p_2, \cdots, p_r$ の中に mod 4 で 3 となるものが s 個あれば，s 個以外の p_i は $p_i\equiv 1 \pmod{4}$ であるから

$$(1)\qquad \left(\frac{-1}{m}\right)=\left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_r}\right)=(-1)^s$$

となる．また

$$(2)\qquad \begin{aligned}m&=p_1p_2\cdots p_r\\&\equiv(-1)^s \pmod{4}\end{aligned}$$

となる．s が偶数のときは(1)から $\left(\dfrac{-1}{m}\right)=1$ となり，(2)から $m\equiv 1 \pmod{4}$ となる．s が奇数のときは(1)から $\left(\dfrac{-1}{m}\right)=-1$ となり，(2)から $m\equiv -1 \pmod{4}$ となる．まとめると

$$\left(\frac{-1}{m}\right)=\begin{cases}1, & m\equiv 1 \pmod{4}\text{の場合}\\-1, & m\equiv -1 \pmod{4}\text{の場合}\end{cases}$$

となり，m が素数でなくとも第1補充法則が成り立つ.

次に第2補充法則であるが，$p_1, p_2, \cdots, p_r$ の中に mod 8 で 3 または -3 と合同になる素数が s 個あったとすると，他の素数は mod 8 で 1 または -1 と合同である．よって

$$\left(\frac{2}{m}\right)=\left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_r}\right) = (-1)^s \tag{3}$$

となる．また

$$m \equiv (\pm 3)^s \cdot (\pm 1) \pmod 8 \tag{4}$$

となる．s が偶数ならば(3)から $\left(\dfrac{2}{m}\right)=1$ となり，(4)から $3^2 \equiv 1 \pmod 8$ を使えば $m \equiv \pm 1 \pmod 8$ となる．s が奇数ならば(3)から $\left(\dfrac{2}{m}\right)=-1$ となり，(4)から $m \equiv \pm 3 \pmod 8$ となる．まとめると

$$\left(\frac{2}{m}\right)=\begin{cases} 1, & m \equiv \pm 1 \pmod 8 \text{ の場合} \\ -1, & m \equiv \pm 3 \pmod 8 \text{ の場合} \end{cases}$$

となり，m が合成数でも第2補充法則が成り立つ．

次に q を奇素数とする．$q \equiv 1 \pmod 4$ ならばいつも $\left(\dfrac{q}{p_i}\right)=\left(\dfrac{p_i}{q}\right)$ であるから

$$\left(\frac{q}{m}\right)=\left(\frac{q}{p_1}\right)\left(\frac{q}{p_2}\right)\cdots\left(\frac{q}{p_r}\right) = \left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right)\cdots\left(\frac{p_r}{q}\right) = \left(\frac{m}{q}\right)$$

となる．$q \equiv -1 \pmod 4$ のとき $p_i \equiv -1 \pmod 4$ となる素数 p_i が s 個あったとすると

$$\left(\frac{q}{m}\right)=\left(\frac{q}{p_1}\right)\left(\frac{q}{p_2}\right)\cdots\left(\frac{q}{p_r}\right) = (-1)^s\left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right)\cdots\left(\frac{p_r}{q}\right)$$

$$=(-1)^s\left(\frac{m}{q}\right)$$

となる．$m=p_1p_2\cdots p_r\equiv(-1)^s \pmod 4$ だから，s が偶数のときは $m\equiv 1 \pmod 4$ となり，s が奇数のときは $m\equiv -1 \pmod 4$ となる．よって

$$(5)\qquad \left(\frac{q}{m}\right)=\begin{cases}\left(\frac{m}{q}\right), & m\equiv 1 \text{ または } q\equiv 1 \pmod 4\\ -\left(\frac{m}{q}\right), & m\equiv q\equiv -1 \pmod 4\end{cases}$$

となる．n を奇数とし，$n=q_1q_2\cdots q_t$ とすれば

$$\left(\frac{n}{m}\right)=\left(\frac{q_1}{m}\right)\left(\frac{q_2}{m}\right)\cdots\left(\frac{q_t}{m}\right)$$
$$=\pm\left(\frac{m}{q_1}\right)\left(\frac{m}{q_2}\right)\cdots\left(\frac{m}{q_t}\right)$$
$$=\pm\left(\frac{m}{n}\right)$$

ここで(5)から $m\equiv 1 \pmod 4$ ならば符号は正であり，$m\equiv -1 \pmod 4$ のときは $q_i\equiv -1 \pmod 4$ となる個数が偶数または奇数にしたがって正または負になる．つまり $n\equiv 1$ または $n\equiv -1 \pmod 4$ にしたがって正または負となる．まとめると

$$\left(\frac{n}{m}\right)=\begin{cases}\left(\frac{m}{n}\right), & m\equiv 1 \text{ または } n\equiv 1 \pmod 4\\ -\left(\frac{m}{n}\right), & m\equiv n\equiv -1 \pmod 4\end{cases}$$

となる．

例
$$\left(\frac{30}{97}\right)=\left(\frac{2}{97}\right)\left(\frac{15}{97}\right)$$
$$=\left(\frac{15}{97}\right)\qquad \because\quad 97\equiv 1 \pmod 8$$

$$= \left(\frac{97}{15}\right) \qquad \because \quad 97 \equiv 1 \pmod 4$$

$$= \left(\frac{7}{15}\right) \qquad \because \quad 97 \equiv 7 \pmod{15}$$

$$= -\left(\frac{15}{7}\right) \qquad \because \quad 7 \equiv 15 \equiv -1 \pmod 4$$

$$= -\left(\frac{1}{7}\right) \qquad \because \quad 15 \equiv 1 \pmod 7$$

$$= -1. \text{ ——}$$

このように分母，分子が素数でなくとも，奇数ならば強引に計算していくことが出来る.

第8章　ペル方程式

§1　歴　史

フェルマー(1601–1665)は17世紀のフランスの数学者だが，イギリスの数学者に挑戦し

(1)
$$x^2-61y^2=1$$

(2)
$$x^2-109y^2=1$$

などの方程式の自然数解を求めよ，という問題を出した(1657)．同年イギリスのブラウンカーとウォリスは，最小の解を求める計算法を考え出した．後年オイラーもこの問題に興味を持ち，実質的に同じ方法で(1)，(2)を解いた(1753)．答は非常に大きく，最小の解は

$$1766319049^2-61\times226153980^2=1$$

$$158070671986249^2-109\times15140424455100^2=1$$

となる．(1)，(2)の右辺を -1 に変えたものの解は

$$29718^2-61\times3805^2=-1$$

$$8890182^2-109\times851525^2=-1$$

がある．これらの方程式の一般形は，m を平方数ではない自然数としたとき

(3)
$$x^2-my^2=\pm1$$

と書ける．複号は，左辺の値が1または -1 となるような解を求めよ，という意味である．オイラーは"(3)を解く方法を最初に考え出した人はペルである"と誤解したため，オイラー以後，(3)は**ペル方程式**と呼ばれている．ブラウンカー，ウォリス，オイラーの方法は，(3)が解を持てばその解を能率良く計算する方法であるけれど，(3)が必ず解を持つことはラグランジュがはじめて証明した(1766–1767

ごろ).

例　m が小さいとき，(3)を解いてみよう．(3)は

(4) $$x^2 \pm 1 = my^2$$

となるから，x の小さい順に(4)の左辺を計算してみよう．

表 8-1

x	x^2	x^2-1	x^2+1	x	x^2	x^2-1	x^2+1
1	1	0	2	6	36	35	37
2	4	3	5	7	49	48	50
3	9	8	10	8	64	63	65
4	16	15	17	9	81	80	82
5	25	24	26	10	100	99	101

$m=2, 3, 5, \cdots$ に対して my^2 を y の小さい順に計算し，表 8-1 と比べてみると

表 8-2

m	my^2	x^2-my^2
2	$2\cdot1^2=2$	$1^2-2\cdot1^2=-1$
3	$3\cdot1^2=3$	$2^2-3\cdot1^2=1$
5	$5\cdot1^2=5$	$2^2-5\cdot1^2=-1$
6	$6\cdot2^2=24$	$5^2-6\cdot2^2=1$
7	$7\cdot3^2=63$	$8^2-7\cdot3^2=1$
8	$8\cdot1^2=8$	$3^2-8\cdot1^2=1$

となり，最小の自然数解が求まった．——

この例のように，すべての可能性を計算して解く方法では，フェルマーの挑戦に応ずることが出来ない．この章では，実質的にはユークリッドの互除法と同じ算法で，ペル方程式が解けることと，ディリクレの部屋割り論法を使って，必ず解があることを示そう．

§2　2次数 $x+y\sqrt{m}$ の性質

さて，ペル方程式

$$x^2-my^2 = \pm 1 \qquad (m\text{ は平方数でない自然数})$$

を解くには，因数分解して

$$(x+y\sqrt{m})(x-y\sqrt{m}) = \pm 1$$

を解けばよい．そのためには $x+y\sqrt{m}$ という形をした数の性質を調べる必要がある．まず $\sqrt{m}$ が無理数であることを示そう．

もし $\sqrt{m}$ が有理数として $\sqrt{m}=\dfrac{a}{b}$ (a, b は自然数) となったとする．m, a, b のどれかを割る素数を $p_1, p_2, \cdots, p_r$ とし，m, a, b は次のように素因子分解したとする．

$$m = p_1{}^{e_1}\cdot p_2{}^{e_2}\cdot\cdots\cdot p_r{}^{e_r} \qquad (e_i \geqq 0)$$
$$a = p_1{}^{f_1}\cdot p_2{}^{f_2}\cdot\cdots\cdot p_r{}^{f_r} \qquad (f_i \geqq 0)$$
$$b = p_1{}^{g_1}\cdot p_2{}^{g_2}\cdot\cdots\cdot p_r{}^{g_r} \qquad (g_i \geqq 0).$$

$\sqrt{m}=\dfrac{a}{b}$ の両辺を自乗すると $mb^2=a^2$ が得られるが，この両辺を素因子分解すると，

$$p_1{}^{e_1+2g_1}\cdot p_2{}^{e_2+2g_2}\cdot\cdots\cdot p_r{}^{e_r+2g_r} = p_1{}^{2f_1}\cdot p_2{}^{2f_2}\cdot\cdots\cdot p_r{}^{2f_r}$$

となる．m が平方数でないから，$e_1, e_2, \cdots, e_r$ のどれかは奇数である．よって素因子分解の一意性に反する．まとめると次の補題となる．

補題1　m を平方数でない自然数とすると，$\sqrt{m}$ は無理数である．

——

この補題を利用すると

(1)　　$a+b\sqrt{m} = 0 \Longrightarrow a=b=0 \qquad (a, b\text{ は有理数})$

が出てくる．なぜならば，もし $b=0$ ならば，

$$a = a+b\sqrt{m} = 0$$

となり $a=b=0$ が得られる．$b\neq 0$ ならば

$$a+b\sqrt{m}=0, \qquad \therefore \quad \sqrt{m}=-\frac{a}{b}$$

となり $\sqrt{m}$ が有理数になって矛盾である．よって(1)が得られた．

さて，(1)を利用すると，a, b, c, d が有理数のとき，

(2)　$$a+b\sqrt{m}=c+d\sqrt{m} \Longrightarrow a=c, b=d$$

が得られる．なぜならば，移項すると

$$(a-c)+(b-d)\sqrt{m}=0$$

となるので $a-c=0$, $b-d=0$ となるからである．$a+b\sqrt{m}$ という表わし方は1通りしかないのである．まとめると

補題2　a, b, c, d を有理数とすると

$$a+b\sqrt{m}=0 \Longrightarrow a=b=0$$

$$a+b\sqrt{m}=c+d\sqrt{m} \Longrightarrow a=c, \quad b=d. \text{ ——}$$

さて $a+b\sqrt{m}$ の形の数を足しても引いても，掛けても割っても，同じ形をしている．すなわち $\alpha=a+b\sqrt{m}$，$\beta=c+d\sqrt{m}$ のとき

(3)　$$\begin{aligned}\alpha+\beta &= (a+b\sqrt{m})+(c+d\sqrt{m}) \\ &= (a+c)+(b+d)\sqrt{m}\end{aligned}$$

(4)　$$\begin{aligned}\alpha-\beta &= (a+b\sqrt{m})-(c+d\sqrt{m}) \\ &= (a-c)+(b-d)\sqrt{m}\end{aligned}$$

(5)　$$\begin{aligned}\alpha\cdot\beta &= (a+b\sqrt{m})\cdot(c+d\sqrt{m}) \\ &= ac+ad\sqrt{m}+bc\sqrt{m}+bd(\sqrt{m})^2 \\ &= (ac+bdm)+(ad+bc)\sqrt{m}\end{aligned}$$

となり，割り算については $\beta\neq 0$ のとき $c+d\sqrt{m}\neq 0$ から $c\neq 0$ または $d\neq 0$ である．このとき $c-d\sqrt{m}\neq 0$ である．なぜなら補題2から，c または d が0でなければ $c-d\sqrt{m}\neq 0$ となるわけである．このとき

$$\begin{aligned}(c+d\sqrt{m})(c-d\sqrt{m}) &= c^2-(d\sqrt{m})^2 \\ &= c^2-d^2m\end{aligned}$$

を利用すると

$$\frac{\alpha}{\beta}=\frac{a+b\sqrt{m}}{c+d\sqrt{m}} \tag{6}$$

$$=\frac{(a+b\sqrt{m})(c-d\sqrt{m})}{(c+d\sqrt{m})(c-d\sqrt{m})}$$

$$=\frac{(ac-bdm)+(-ad+bc)\sqrt{m}}{c^2-d^2m}$$

$$=\frac{ac-bdm}{c^2-d^2m}+\frac{-ad+bc}{c^2-d^2m}\sqrt{m}$$

となる．よって次の補題が得られる．

補題 3　a, b, c, d が有理数，$\alpha=a+b\sqrt{m}$，$\beta=c+d\sqrt{m}$ のとき，$\alpha+\beta$, $\alpha-\beta$, $\alpha\cdot\beta$, α/β ($\beta\neq 0$ のとき) はやはり有理数＋有理数×$\sqrt{m}$ という形をしている．——

例　$\alpha=3+2\sqrt{5}$，$\beta=2+3\sqrt{5}$ のとき

$$\alpha+\beta=5+5\sqrt{5}$$

$$\alpha-\beta=1-\sqrt{5}$$

$$\alpha\cdot\beta=(6+30)+(9+4)\sqrt{5}$$

$$=36+13\sqrt{5}$$

$$\frac{\alpha}{\beta}=\frac{(3+2\sqrt{5})(2-3\sqrt{5})}{(2+3\sqrt{5})(2-3\sqrt{5})}$$

$$=\frac{(6-30)+(-9+4)\sqrt{5}}{-41}$$

$$=\frac{24}{41}+\frac{5}{41}\sqrt{5}.$$ ——

次に $\alpha=a+b\sqrt{m}$ に対して $\alpha'=a-b\sqrt{m}$ と定義して α' を α の**共役元**と呼ぶ．複素数 $\alpha=a+b\sqrt{-1}$ に対して複素共役を $\bar{\alpha}=a-b\sqrt{-1}$ と定義するのと同じである．共役元の共役元は元にもどる．つまり

$$\alpha''=(\alpha')'=(a-b\sqrt{m})'=a-(-b)\sqrt{m}$$

$$= a+b\sqrt{m} = \alpha$$

となる．また $b=0$ のとき，つまり $\alpha=a+0\sqrt{m}=a=$有理数 に対しては $\alpha'=a-0\sqrt{m}=a=\alpha$ となる．逆に $\alpha=a+b\sqrt{m}$ に対して $\alpha=\alpha'$ ならば

$$a+b\sqrt{m} = a-b\sqrt{m}$$

から $2b\sqrt{m}=0$ となり $b=0$ が得られ，$\alpha=$有理数 となる．まとめると

補題 4 $\alpha'' = \alpha$

$\alpha' = \alpha \Longleftrightarrow \alpha =$ 有理数．——

四則算法を行うことと，共役元を作ることは，どちらを先にしても結果は同じである．$\alpha=a+b\sqrt{m}$，$\beta=c+d\sqrt{m}$ のとき，前に得た四則算法の式を使うと

$$\begin{aligned}\alpha'+\beta' &= (a-b\sqrt{m})+(c-d\sqrt{m})\\ &= (a+c)-(b+d)\sqrt{m}\\ &= (\alpha+\beta)'\\ \alpha'-\beta' &= (a-b\sqrt{m})-(c-d\sqrt{m})\\ &= (a-c)-(b-d)\sqrt{m}\\ &= (\alpha-\beta)'\\ \alpha'\cdot\beta' &= (a-b\sqrt{m})(c-d\sqrt{m})\\ &= (ac+bdm)-(ad+bc)\sqrt{m}\\ &= (\alpha\cdot\beta)'.\end{aligned}$$

割り算については，掛け算の結果を利用すると，

$$\left(\frac{\alpha}{\beta}\right)'\cdot\beta' = \left\{\left(\frac{\alpha}{\beta}\right)\cdot\beta\right\}' = \alpha'$$

$$\therefore \quad \left(\frac{\alpha}{\beta}\right)' = \frac{\alpha'}{\beta'}$$

となる．よって次のようにまとめられる．

補題 5　四則算法を行うことと，共役元を作ることはどちらを先にしても結果は同じである．——

この結果を何回も使えば，たとえば

$$
\begin{aligned}
(\alpha^n)' &= (\alpha^{n-1}\cdot\alpha)' = (\alpha^{n-1})'\cdot\alpha' \\
&= (\alpha^{n-2}\cdot\alpha)'\cdot\alpha' = (\alpha^{n-2})'\cdot\alpha'\cdot\alpha' \\
&\cdots \\
&= (\alpha')^n
\end{aligned}
$$

となる．

さて，x, y, u, v を整数とし，$\alpha=x+y\sqrt{m}$，$\beta=u+v\sqrt{m}$ のとき $\alpha+\beta, \alpha-\beta, \alpha\cdot\beta$ は(3)，(4)，(5)から 整数＋整数×$\sqrt{m}$ という形をしている．また $\alpha\alpha'=(x+y\sqrt{m})(x-y\sqrt{m})=x^2-my^2=$整数 となる．特にペル方程式は $\alpha\alpha'=\pm1$ となる α を求めることである．

ところで自然数 x, y に対し $\alpha=x+y\sqrt{m}$ が $\alpha\alpha'=\pm1$ のとき，2項定理から

$$
\begin{aligned}
\alpha^n &= (x+y\sqrt{m})^n \\
&= x^n+\binom{n}{1}x^{n-1}\cdot y\sqrt{m}+\binom{n}{2}x^{n-2}\cdot y^2(\sqrt{m})^2+\cdots \\
&= \left(x^n+\binom{n}{2}x^{n-2}\cdot y^2\cdot m+\cdots\right) \\
&\quad +\left(\binom{n}{1}x^{n-1}\cdot y+\binom{n}{3}x^{n-3}y^3m+\cdots\right)\sqrt{m}
\end{aligned}
$$

となるので

$$\alpha^n = x_n+y_n\sqrt{m}$$

とおくことが出来る．x_n, y_n はやはり自然数である．このとき

$$
\begin{aligned}
{x_n}^2-m{y_n}^2 &= (x_n+y_n\sqrt{m})(x_n-y_n\sqrt{m}) \\
&= \alpha^n\cdot(\alpha^n)' \\
&= \alpha^n\cdot(\alpha')^n
\end{aligned}
$$

$$= (\alpha\cdot\alpha')^n$$
$$= (\pm 1)^n$$

となる．つまり x_n, y_n の組合せもペル方程式の解となる．すなわち1つでも解があれば，無限に解がある．

例　$m=5$ のとき

$$2^2-5\cdot 1^2 = -1$$

が最小の解である．$\alpha=2+\sqrt{5}$ とおくと

$$\alpha^2 = 4+4\sqrt{5}+5$$
$$= 9+4\sqrt{5}$$

であるから

$$9^2-5\cdot 4^2 = (\alpha\alpha')^2 = 1$$

となる．——

例　$m=61$ のとき，最小の解

$$29718^2-61\cdot 3805^2 = -1$$

が求まったとする．このとき

$$(29718+3805\sqrt{61})^2$$
$$= 29718^2+3805^2\cdot 61+2\cdot 29718\cdot 3805\cdot\sqrt{61}$$
$$= 1766319049+226153980\sqrt{61}$$

から

$$1766319049^2-61\cdot 226153980^2 = (-1)^2 = 1$$

が得られる．——

§3　格子点

X-Y 平面において X 座標が $\alpha=x+y\sqrt{m}$，Y 座標が $\alpha'=x-y\sqrt{m}$ となる点 $\boldsymbol{P}=(\alpha,\alpha')$ を考えてみよう．最大公約数を表わす記号と同じになってしまったが，この章で使う記号 (α,β) は X 座標が α，Y 座標が β という点を表わす記号である．点を表わすというよ

りも，原点からのベクトルを表わす，と思うこともできる．よって同じ記号(α, α')で点を表わすことと，原点からのベクトルを表わすこととの2通りの意味がある．ベクトル演算で書くと

(1)　$(\alpha, \alpha') = (x+y\sqrt{m}, x-y\sqrt{m}) = x(1,1)+y(\sqrt{m}, -\sqrt{m})$

となる．$\alpha_0=1$，$\alpha_{-1}=\sqrt{m}$，$\boldsymbol{\alpha}=(\alpha, \alpha')$，$\boldsymbol{\alpha}_0=(\alpha_0, \alpha_0')=(1,1)$，$\boldsymbol{\alpha}_{-1}=(\alpha_{-1}, \alpha_{-1}')=(\sqrt{m}, -\sqrt{m})$とおくと(1)は

(2)　$$\boldsymbol{\alpha} = x\boldsymbol{\alpha}_0 + y\boldsymbol{\alpha}_{-1}$$

となる．図8-1は$m=5$のときの図である．

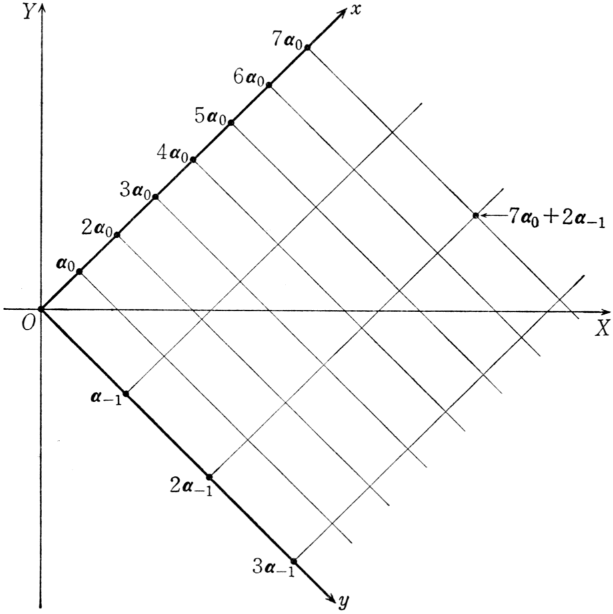


図 8-1

x, yを整数としたとき，(2)のように表わされる点$\boldsymbol{\alpha}$を**格子点**と呼ぶことにしよう．(前章の格子点は$\boldsymbol{\alpha}_0=(1,0)$，$\boldsymbol{\alpha}_{-1}=(0,1)$という

場合である.) 格子点全体を $\boldsymbol{L}$ としたとき, $\boldsymbol{L}$ のどの元も(2)から $\boldsymbol{\alpha}_0$ の整数倍と $\boldsymbol{\alpha}_{-1}$ の整数倍との和として表わされる. このようなとき, $\boldsymbol{L}$ の元は $\boldsymbol{\alpha}_0$ と $\boldsymbol{\alpha}_{-1}$ の整数係数の**1次結合**で書ける, という. また, このような性質を持つ $\boldsymbol{\alpha}_0, \boldsymbol{\alpha}_{-1}$ のことを $\boldsymbol{L}$ の**生成元**という. 集合論の記号を使えば

$$\boldsymbol{L} = \{x\boldsymbol{\beta}+y\boldsymbol{\gamma} \mid x, y \text{ は整数}\}$$

となるとき, $\boldsymbol{\beta}$ と $\boldsymbol{\gamma}$ を $\boldsymbol{L}$ の生成元という. 生成元はいろいろな組合せがある. たとえば $\boldsymbol{\beta}$ と $\boldsymbol{\gamma}$ が $\boldsymbol{L}$ の生成元, k=整数 のとき, $\boldsymbol{\gamma}$ と $\boldsymbol{\delta}=\boldsymbol{\beta}+k\boldsymbol{\gamma}$ も $\boldsymbol{L}$ の生成元である. なぜならば

$$\boldsymbol{\beta} = (\boldsymbol{\beta}+k\boldsymbol{\gamma})+(-k)\boldsymbol{\gamma} = \boldsymbol{\delta}+(-k)\boldsymbol{\gamma}$$

であるから

$$\begin{aligned} x\boldsymbol{\beta}+y\boldsymbol{\gamma} &= x(\boldsymbol{\delta}+(-k)\boldsymbol{\gamma})+y\boldsymbol{\gamma} \\ &= (-xk+y)\boldsymbol{\gamma}+x\boldsymbol{\delta} \end{aligned}$$

となり, $\boldsymbol{L}$ の元はすべて $\boldsymbol{\gamma}$ と $\boldsymbol{\delta}$ の整数係数の1次結合で書ける. 逆に $\boldsymbol{\gamma}$ と $\boldsymbol{\delta}$ の整数係数の1次結合は

$$\begin{aligned} x\boldsymbol{\gamma}+y\boldsymbol{\delta} &= x\boldsymbol{\gamma}+y(\boldsymbol{\beta}+k\boldsymbol{\gamma}) \\ &= y\boldsymbol{\beta}+(x+yk)\boldsymbol{\gamma} \end{aligned}$$

であるから $\boldsymbol{L}$ の元である.

よって次のようにまとめられる.

補題6 $\boldsymbol{\beta}$ と $\boldsymbol{\gamma}$ が $\boldsymbol{L}$ の生成元, k が整数のとき, $\boldsymbol{\gamma}$ と $\boldsymbol{\delta}=\boldsymbol{\beta}+k\boldsymbol{\gamma}$ も $\boldsymbol{L}$ の生成元である. ——

$\boldsymbol{L}$ の元 $\boldsymbol{\alpha}=(\alpha, \alpha')$ が X 軸上にあるのは $\alpha'=0$ のときである. よって $\alpha=(\alpha')'=0'=0$ となり, 原点以外の $\boldsymbol{L}$ の元は X 軸上にはない.

さて, 図8-2を見よう. $\boldsymbol{\beta}=(\beta, \beta')$ と $\boldsymbol{\gamma}=(\gamma, \gamma')$ が $\boldsymbol{L}$ の生成元で $0<\beta, 0<\gamma, 0<\gamma'<-\beta'$ とする. このとき $\overrightarrow{OC}$ に平行に B から直線を引くと, X 軸とぶつかるところをベクトルで表わすと $\boldsymbol{\beta}+\left(-\dfrac{\beta'}{\gamma'}\right)\boldsymbol{\gamma}$ である. なぜならば B から X 軸までの長さは, Y 座標 β' の絶対値

$-\beta'$ であり，C から X 軸までの長さは γ' である．図8-2において三角形 BDF は三角形 CEO と相似だから

$$\overrightarrow{BF} = \left(\frac{-\beta'}{\gamma'}\right)\cdot\overrightarrow{OC} = \frac{-\beta'}{\gamma'}\boldsymbol{\gamma}$$

となるからである．よってその直前の格子点は

(1)
$$\boldsymbol{\varepsilon} = \boldsymbol{\beta} + \left[\frac{-\beta'}{\gamma'}\right]\cdot\boldsymbol{\gamma}$$

となる．また補題6から $\boldsymbol{\gamma}$ と $\boldsymbol{\varepsilon}$ は $\boldsymbol{L}$ の生成元となる．

ところで $\boldsymbol{\varepsilon}$ には次の性質がある．$\boldsymbol{L}$ の元 $\boldsymbol{\delta}=(\delta, \delta')$ で $\gamma<\delta, |\delta'|<\gamma'$ であり δ が最小となるものは $\boldsymbol{\delta}=\boldsymbol{\varepsilon}$ となる．図8-3において斜線を引いた部分が，X 座標が γ より大きく Y 座標の絶対値が γ' より小さくなる領域である．この中最初の，つまり X 座標が最小な $\boldsymbol{L}$ の元

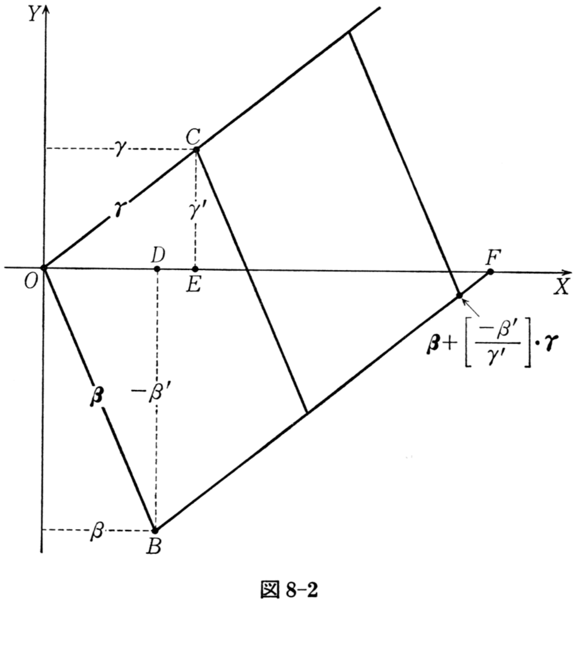


図8-2

が(1)で与えられる．この事実は図8-3からほぼ明らかであるが，少し説明を加えると次のようになる．

$$\boldsymbol{\delta} = x\boldsymbol{\gamma}+y\boldsymbol{\beta}$$

とおく．もし $y\leqq 0$ ならば $\boldsymbol{\delta}$ は図8-3において直線 AB の左上になるから，斜線の部分には来ない．$y=1$ ならば $x=\left[\dfrac{-\beta'}{\gamma'}\right]$ となる．x の値をこのままで，y の値を大きくすると直線 CD の下，つまり斜線の部分の下になってしまうので，$y\geqq 2$ のとき斜線の内部に $\boldsymbol{\delta}$ を入れようとすると，x の値も増やさなければならない．x の値も y の値も同時に大きくなれば $\delta=x\gamma+y\beta$ も大きくなるので，(1)が最小な δ の値を与える．

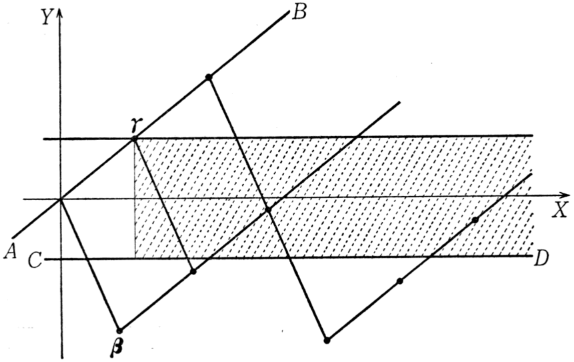


図8-3

以上の説明は $0<\gamma'<-\beta'$ であったが，$0>\gamma'>-\beta'$ でも X 軸を中心に上下が逆になるだけであるから，同様の結果を得る．まとめると次のようになる．

補題7 $\boldsymbol{\beta}=(\beta,\beta')$, $\boldsymbol{\gamma}=(\gamma,\gamma')$ が $\boldsymbol{L}$ の生成元で $0<\beta, 0<\gamma, \beta'\cdot\gamma'<0$, $|\gamma'|<|\beta'|$ とする．このとき $\boldsymbol{L}$ の元 $\boldsymbol{\delta}=(\delta,\delta')$ で $\gamma<\delta$, $|\delta'|<|\gamma'|$ であり，δ が最小となる元は

$$\boldsymbol{\delta} = \boldsymbol{\beta} + \left[-\frac{\beta'}{\gamma'} \right] \boldsymbol{\gamma}$$

である．このとき $\boldsymbol{\gamma}$ と $\boldsymbol{\delta}$ の組合せは，$\boldsymbol{\beta}$ と $\boldsymbol{\gamma}$ の組合せと同じ性質を持っている．すなわち $\boldsymbol{\gamma}$ と $\boldsymbol{\delta}$ は $\boldsymbol{L}$ の生成元で，$0<\gamma, 0<\delta, \gamma'\cdot\delta'<0$, $|\delta'|<|\gamma'|$ となる．——

§4 連分数展開

ペル方程式 $x^2-my^2=\pm1$ の2組の解 x_1, y_1 と x_2, y_2 があったとしよう．$x_1{}^2-my_1{}^2=x_2{}^2-my_2{}^2$ ならば $x_1<x_2 \Longleftrightarrow y_1<y_2$ はすぐ言える．しかし片方が -1 で他方が1であったとしても，$x_1<x_2$ ならば

$$\begin{aligned} my_1{}^2 &= x_1{}^2\pm1 \leqq x_1{}^2+1 = x_1{}^2+2x_1+1-2x_1 \\ &< (x_1+1)^2-1 \leqq x_2{}^2-1 \leqq my_2{}^2 \end{aligned}$$

であるから $y_1<y_2$ が得られる．逆に $y_1<y_2$ ならば

$$\begin{aligned} x_1{}^2 &= my_1{}^2\pm1 \leqq my_1{}^2+1 = m(y_1{}^2+2y_1+1)-(2my_1+m-1) \\ &< m(y_1+1)^2-1 \leqq my_2{}^2-1 \leqq x_2{}^2 \end{aligned}$$

であるから $x_1<x_2$ が得られる．次に

$$x_1+y_1\sqrt{m} < x_2+y_2\sqrt{m}$$

のとき $x_1<x_2$ または $y_1<y_2$ でなければならない．どちらが成り立っても他方も成り立つので，次の補題が得られた．

補題 8 $x_1{}^2-my_1{}^2=\pm1$，$x_2{}^2-my_2{}^2=\pm1$ のとき

$$\begin{aligned} x_1 < x_2 &\Longleftrightarrow y_1 < y_2 \\ &\Longleftrightarrow x_1+y_1\sqrt{m} < x_2+y_2\sqrt{m}. \text{ ——} \end{aligned}$$

よって**最小の解を見つける**ということは，x が最小の解を見つけることでもあり，y が最小な解を見つけることでもあり，$\alpha=x+y\sqrt{m}$ が最小な解を見つけることでもある．

さて $\alpha\alpha'=\pm1$ となる α を見つけるということは格子点の中で X

座標と Y 座標の積が 1 または -1 となる点を見つけることである．どのようにすべての解を見つけるか素朴に考えてみよう．

x, y が自然数のときは $\alpha=x+y\sqrt{m}>1$ となる．$\alpha\alpha'=\pm 1$ であったとしよう．このとき $\alpha>1$ から

$$1=|\alpha\alpha'|=\alpha|\alpha'|>|\alpha'|$$

となる．よって $1<\alpha_1, |\alpha_1{}'|<1$ となる最小の α_1 はどのような数になるか考えるのは自然であろう．$\boldsymbol{\beta}=\boldsymbol{\alpha}_{-1}=(\sqrt{m}, -\sqrt{m})$, $\boldsymbol{\gamma}=\boldsymbol{\alpha}_0=(1, 1)$ とおけば $\boldsymbol{\beta}, \boldsymbol{\gamma}$ は $\boldsymbol{L}$ の生成元であり，$0<\sqrt{m}=\beta$, $0<1=\gamma$, $\beta'=-\sqrt{m}$ と $\gamma'=1$ は異符号，$|\gamma'|=1<\sqrt{m}=|\beta'|$ であるから補題 7 が使える．$1=\gamma<\alpha_1$, $|\alpha_1{}'|<|\gamma'|=1$ となる最小の α_1 はこの補題から

$$\alpha_1=\beta+\left[-\frac{\beta'}{\gamma'}\right]\gamma=\sqrt{m}+[\sqrt{m}]$$

となる．もし $\alpha\neq\alpha_1$ ならば α_1 が $1<\alpha_1$, $|\alpha_1{}'|<1$ となる最小の数であったから $\alpha_1<\alpha$ となる．$\alpha_1\cdot\alpha_1{}'$ は整数であり，$\alpha_1\neq 0$ であるから $\alpha_1{}'\neq 0$ となり $1\leqq|\alpha_1\alpha_1{}'|$ となる．よって $\alpha_1<\alpha$ と $1=\alpha|\alpha'|\leqq|\alpha_1\alpha_1{}'|=\alpha_1|\alpha_1{}'|$ から $|\alpha'|\leqq\left(\dfrac{\alpha_1}{\alpha}\right)\cdot|\alpha_1{}'|<|\alpha_1{}'|$ となる．$\alpha_1<\alpha_2$, $|\alpha_2{}'|<|\alpha_1{}'|$ となる最小な α_2 はどうなるか考えてみよう．

$\boldsymbol{\beta}=\boldsymbol{\alpha}_0, \boldsymbol{\gamma}=\boldsymbol{\alpha}_1=(\alpha_1, \alpha_1{}')$ とおくと補題 7 の後半から $\boldsymbol{\beta}, \boldsymbol{\gamma}$ は補題 7 の条件を満たす．よって $\alpha_1=\gamma<\alpha_2, |\alpha_1{}'|=|\gamma'|>|\alpha_2{}'|$ となる最小の α_2 は

$$\alpha_2=\beta+\left[-\frac{\beta'}{\gamma'}\right]\gamma=\alpha_0+\left[-\frac{\alpha_0{}'}{\alpha_1{}'}\right]\alpha_1$$

となる．もし $\alpha\neq\alpha_2$ ならば同じ操作を続ければよい．すなわち

$$\alpha_{i+1}=\alpha_{i-1}+\left[-\frac{\alpha_{i-1}{}'}{\alpha_i{}'}\right]\alpha_i \tag{1}$$

とおくと

$$1=\alpha_0<\alpha_1<\alpha_2<\cdots \tag{2}$$

(3) $$\sqrt{m}=|\alpha_{-1}'|>1=|\alpha_0'|>|\alpha_1'|>\cdots$$

となる数列が出来, α は数列(2)の中に必ず現われるはずである．よってペル方程式のすべての解は(2)の中にある．また α_{i-1}' と α_i' は異符号であり，$\alpha_0'=1$ であるから

(4) $$\alpha_i'=(-1)^i|\alpha_i'|$$

となる．$\beta_i=-\dfrac{\alpha_{i-1}'}{\alpha_i'}$，$k_i=[\beta_i]$ とおくと

$$\beta_0=-\frac{\alpha_{-1}'}{\alpha_0'}=-\frac{-\sqrt{m}}{1}=\sqrt{m}$$

となり(1)は

(5) $$\alpha_{i+1}=\alpha_{i-1}+k_i\alpha_i$$

となる．(5)から

$$\begin{aligned}\alpha_{i+1}'&=(\alpha_{i-1}+k_i\alpha_i)'=\alpha_{i-1}'+(k_i\alpha_i)'\\&=\alpha_{i-1}'+k_i'\alpha_i'=\alpha_{i-1}'+k_i\alpha_i'\end{aligned}$$

であるから β_{i+1} は

(6) $$\begin{aligned}\beta_{i+1}&=-\frac{\alpha_i'}{\alpha_{i+1}'}=-\frac{\alpha_i'}{\alpha_{i-1}'+k_i\alpha_i'}\\&=\frac{1}{-\alpha_{i-1}'/\alpha_i'-k_i}\\&=\frac{1}{\beta_i-k_i}\end{aligned}$$

となる．つまり β_{i+1} は β_i の小数部の逆数である．この式から $\beta_i-k_i=\dfrac{1}{\beta_{i+1}}$，つまり

(7) $$\beta_i=k_i+\frac{1}{\beta_{i+1}}$$

となる．$\beta_0=\sqrt{m}$ であるから

$$\sqrt{m}=\beta_0=k_0+\frac{1}{\beta_1}$$

$$= k_0 + \cfrac{1}{k_1 + \cfrac{1}{\beta_2}}$$

$$\cdots$$

$$= k_0 + \cfrac{1}{k_1 + \cfrac{1}{k_2 + \ddots + \cfrac{1}{k_{n-1} + \cfrac{1}{\beta_n}}}}$$

となる．この式を $\sqrt{m}$ の**連分数展開**という．

§5　いくつかの例

ペル方程式 $x^2-7y^2=\pm1$ を解いてみよう．

$$\beta_0 = \sqrt{7} = 2.6\cdots, \qquad k_0 = 2$$

$$\beta_1 = \frac{1}{\sqrt{7}-2} = \frac{\sqrt{7}+2}{3} = 1.5\cdots, \qquad k_1 = 1$$

$$\beta_2 = \frac{1}{(\sqrt{7}+2)/3-1}$$

$$= \frac{3}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{2} = 1.8\cdots, \qquad k_2 = 1$$

$$\beta_3 = \frac{1}{(\sqrt{7}+1)/2-1}$$

$$= \frac{2}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{3} = 1.2\cdots, \qquad k_3 = 1$$

$$\beta_4 = \frac{1}{(\sqrt{7}+1)/3-1}$$

$$= \frac{3}{\sqrt{7}-2} = \frac{\sqrt{7}+2}{1}.$$

このように β_i を計算していくと，β_4 の分母が 1 となった．実は次節で証明するけれど，或る整数 a_i が定まって $\beta_i = \dfrac{\sqrt{m}+a_i}{|\alpha_i\alpha_i'|}$ となる．よって α_4 が最小な解となる．α_i を計算すると(図 8-4 参照)

$$\alpha_{-1} = \sqrt{7}$$
$$\alpha_0 = 1$$
$$\alpha_1 = \alpha_{-1}+k_0\alpha_0 = \sqrt{7}+2$$
$$\alpha_2 = \alpha_0+k_1\alpha_1 = 1+(\sqrt{7}+2) = \sqrt{7}+3$$
$$\alpha_3 = \alpha_1+k_2\alpha_2 = (\sqrt{7}+2)+(\sqrt{7}+3) = 2\sqrt{7}+5$$
$$\alpha_4 = \alpha_2+k_3\alpha_3 = (\sqrt{7}+3)+(2\sqrt{7}+5) = 3\sqrt{7}+8.$$

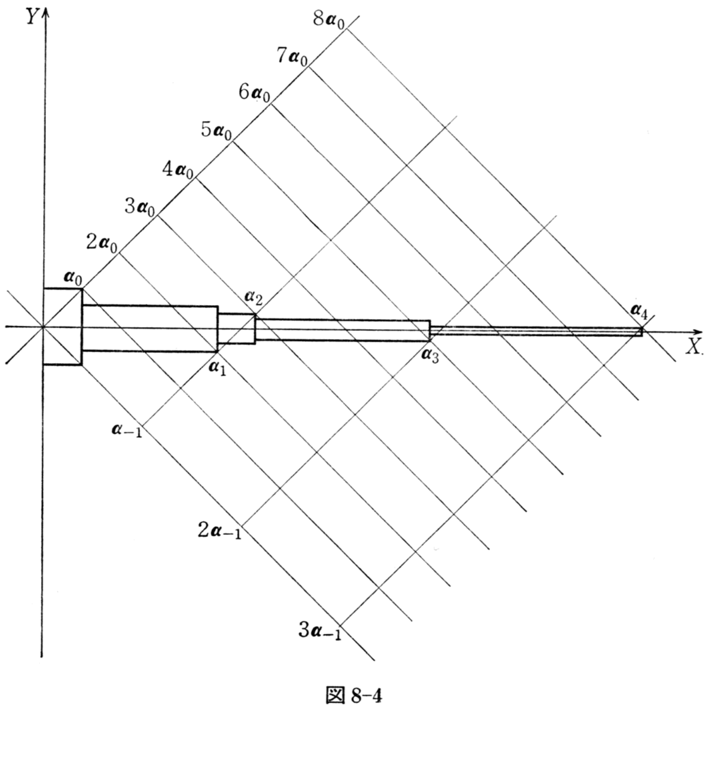


図 8-4

よって $x=8, y=3$ が最小な解となる．検算すると

$$8^2-7\cdot 3^2 = 64-7\cdot 9 = 1$$

となる．$\alpha_4'>0$ であるから $\alpha_4\alpha_4'=1$ となり，検算結果と一致する．

次に，$x^2-19y^2=\pm 1$ を解いてみよう．前と同様に計算していくと

$$\beta_0 = \sqrt{19} = 4.\cdots$$
$$\beta_1 = (\sqrt{19}+4)/3 = 2.\cdots$$
$$\beta_2 = (\sqrt{19}+2)/5 = 1.\cdots$$
$$\beta_3 = (\sqrt{19}+3)/2 = 3.\cdots$$
$$\beta_4 = (\sqrt{19}+3)/5 = 1.\cdots$$
$$\beta_5 = (\sqrt{19}+2)/3 = 2.\cdots$$
$$\beta_6 = (\sqrt{19}+4)/1.$$

このとき α_i も同様に計算していくと

$$\alpha_6 = 170+39\sqrt{19}$$

となる．よって $x=170, y=39$ が最小な解である．また $\alpha_6'>0$ であるから

$$170^2-19\cdot 39^2 = \alpha_6\alpha_6' = 1$$

となる．

次に，フェルマーが出した問題 $x^2-61y^2=\pm 1$ を解こう．

$$\beta_0 = \sqrt{61} = 7.\cdots$$
$$\beta_1 = (\sqrt{61}+7)/12 = 1.\cdots$$
$$\beta_2 = (\sqrt{61}+5)/3 = 4.\cdots$$
$$\beta_3 = (\sqrt{61}+7)/4 = 3.\cdots$$
$$\beta_4 = (\sqrt{61}+5)/9 = 1.\cdots$$
$$\beta_5 = (\sqrt{61}+4)/5 = 2.\cdots$$
$$\beta_6 = (\sqrt{61}+6)/5 = 2.\cdots$$
$$\beta_7 = (\sqrt{61}+4)/9 = 1.\cdots$$

$$\beta_8 = (\sqrt{61}+5)/4 = 3.\cdots$$
$$\beta_9 = (\sqrt{61}+7)/3 = 4.\cdots$$
$$\beta_{10} = (\sqrt{61}+5)/12 = 1.\cdots$$
$$\beta_{11} = (\sqrt{61}+7)/1$$

となり α_{11} を計算すると

$$\alpha_{11} = 29718+3805\sqrt{61}$$

となるので

$$29718^2-61\cdot 3805^2 = (-1)^{11} = -1$$

となる．

さて以上の例をよく眺めてみると，β_i の整数部である k_i は $m=19$ のとき $k_1\sim k_5$ は 2, 1, 3, 1, 2 となり $m=61$ のとき $k_1\sim k_{10}$ は 1, 4, 3, 1, 2, 2, 1, 3, 4, 1 となる．どちらも逆から読んでも同じ数列が得られる．また $\beta_i=\dfrac{\sqrt{m}+a_i}{b_i}$ とすると $m=19$ のとき $a_1\sim a_6$ は 4, 2, 3, 3, 2, 4 となり $b_0\sim b_6$ は 1, 3, 5, 2, 5, 3, 1 となる．$m=61$ のときは $a_1\sim a_{11}$ は 7, 5, 7, 5, 4, 6, 4, 5, 7, 5, 7 となり $b_0\sim b_{11}$ は 1, 12, 3, 4, 9, 5, 5, 9, 4, 3, 12, 1 となっていてやはり対称である．次にこれらの事実が一般に成り立つことを証明しよう．

§6　オイラーの定理とガロアの定理

§4 の(1), (6)をまとめると

(1) $$\alpha_{-1} = \sqrt{m},\ \ \alpha_0 = 1,\ \ \alpha_{i+1} = \alpha_{i-1}+\left[-\frac{\alpha_{i-1}'}{\alpha_i'}\right]\alpha_i$$

とおき，$\beta_i=-\dfrac{\alpha_{i-1}'}{\alpha_i'}$ とおくと

(2) $$\beta_0 = \sqrt{m}, \qquad \beta_{i+1} = \frac{1}{\beta_i-[\beta_i]}$$

となる．$[\beta_i]=k_i$ とおくと

(3) $$\alpha_{i+1} = \alpha_{i-1}+k_i\alpha_i$$

となる．まず，次の補題を証明しよう．

補題 9 適当な整数 a_i により

(4) $$\alpha_i\alpha_{i-1}' = (-1)^{i-1}(\sqrt{m}+a_i)$$

と書ける．

証明 数学的帰納法で示そう．

$i=0$ のとき左辺は $\alpha_0\alpha_{-1}'=1\cdot(\sqrt{m})'=-\sqrt{m}$ となり，右辺は $(-1)^{0-1}(\sqrt{m}+a_0)=-(\sqrt{m}+a_0)$ となる．よって $a_0=0$ とおけば 左辺＝右辺 となる．

$\alpha_i\alpha_{i-1}'=(-1)^{i-1}(\sqrt{m}+a_i)$ のとき，両辺の共役をとると

$$(\alpha_i\alpha_{i-1}')' = \alpha_i'\cdot\alpha_{i-1}'' = \alpha_i'\alpha_{i-1}$$

$$\{(-1)^{i-1}(\sqrt{m}+a_i)\}' = (-1)^{i-1}(-\sqrt{m}+a_i) = (-1)^i(\sqrt{m}-a_i).$$

よって $\alpha_{i-1}\alpha_i'=(-1)^i(\sqrt{m}-a_i)$ が得られる．(3) を用いると

$$\begin{aligned}\alpha_{i+1}\alpha_i' &= (\alpha_{i-1}+k_i\alpha_i)\alpha_i'\\ &= \alpha_{i-1}\alpha_i'+k_i\alpha_i\alpha_i'\\ &= (-1)^i\{\sqrt{m}-a_i+(-1)^ik_i\alpha_i\alpha_i'\}.\end{aligned}$$

よって $a_{i+1}=-a_i+(-1)^ik_i\cdot\alpha_i\alpha_i'$ とおけば $\alpha_i\alpha_i'$ が整数となるので a_{i+1} も整数となり，$\alpha_{i+1}\alpha_i'=(-1)^i(\sqrt{m}+a_{i+1})$ となる．つまり (4) が示された．——

定理 21 (オイラー, 1765) $\alpha_i\alpha_{i-1}'=(-1)^{i-1}(\sqrt{m}+a_i)$, $b_i=|\alpha_i\alpha_i'|$ とおけば

$$\beta_i = \frac{\sqrt{m}+a_i}{b_i}.$$

証明 §4(4) と $\alpha_i>0$ から

(5) $$\alpha_i\alpha_i' = (-1)^i\alpha_i|\alpha_i'| = (-1)^i|\alpha_i\alpha_i'|$$

となる．よって

$$\beta_i = -\frac{\alpha_{i-1}'}{\alpha_i'} = -\frac{\alpha_i\alpha_{i-1}'}{\alpha_i\alpha_i'}$$

$$= -\frac{(-1)^{i-1}(\sqrt{m}+a_i)}{(-1)^i|\alpha_i\alpha_i'|}$$

$$= \frac{\sqrt{m}+a_i}{|\alpha_i\alpha_i'|}$$

$$= \frac{\sqrt{m}+a_i}{b_i}. \quad ——$$

この定理により $\alpha\alpha'=\pm1$ となる最小の α を求めるには $\beta_1, \beta_2, \cdots$ を計算してゆき，最初に分母が 1 になるものを β_n とすれば $\alpha=\alpha_n$ であることが保証された．このとき n が偶数であれば $\alpha_n\alpha_n'=1$，奇数ならば $\alpha_n\alpha_n'=-1$ となる．次に k_i が対称であること，つまり $k_i=k_{n-i}$ を示そう．

補題 10 $\gamma_i=\dfrac{\alpha_{i+1}}{\alpha_i}$ とおけば

(6) $$[\gamma_i] = k_i \qquad (1\leqq i)$$

(7) $$\gamma_{i-1} = \frac{1}{\gamma_i-[\gamma_i]} \qquad (1\leqq i)$$

(8) $$\gamma_{i+1} = \frac{1}{\gamma_i}+\left[-\frac{1}{\gamma_i'}\right].$$

補題 9 により $\alpha_{i+1}\alpha_i'=(-1)^i(\sqrt{m}+a_{i+1})$ とおくと

(9) $$\gamma_i = \frac{\sqrt{m}+a_{i+1}}{b_i}$$

となる．β_i に対しては

(10) $$\beta_{i-1} = \frac{1}{\beta_i}+\left[-\frac{1}{\beta_i'}\right] \qquad (2\leqq i)$$

が成り立つ．

証明 $\alpha_{i+1}=\alpha_{i-1}+k_i\alpha_i$ であるから，両辺を α_i で割り

(11) $$\gamma_i = \frac{\alpha_{i-1}}{\alpha_i}+k_i$$

となる．$1 \leqq i$ ならば $0<\alpha_{i-1}<\alpha_i$ であるから $0<\dfrac{\alpha_{i-1}}{\alpha_i}<1$ となり，k_i は整数であるから γ_i の整数部は k_i，つまり $[\gamma_i]=k_i$ となる．また(11)から $\gamma_i=\dfrac{1}{\gamma_{i-1}}+k_i$ であるから $\gamma_i-k_i=\dfrac{1}{\gamma_{i-1}}$，つまり(7)が示された．

$$(12)\qquad \beta_{i+1}=-\frac{\alpha_i'}{\alpha_{i+1}'}=-\frac{1}{\alpha_{i+1}'/\alpha_i'}$$
$$=-\frac{1}{(\alpha_{i+1}/\alpha_i)'}=-\frac{1}{\gamma_i'}$$

であるから $k_{i+1}=[\beta_{i+1}]=\left[-\dfrac{1}{\gamma_i'}\right]$ となる．よって(12)の共役を取り i を $i+1$ にすると(2)から

$$\gamma_{i+1}=-\frac{1}{\beta_{i+2}'}=-\beta_{i+1}'+k_{i+1}$$
$$=\frac{1}{\gamma_i}+\left[-\frac{1}{\gamma_i'}\right]$$

となる．よって(8)が示された．

$$\gamma_i=\frac{\alpha_{i+1}}{\alpha_i}=\frac{(-1)^i\alpha_{i+1}\alpha_i'}{(-1)^i\alpha_i\alpha_i'}$$
$$=\frac{\sqrt{m}+a_{i+1}}{|\alpha_i\alpha_i'|}.$$

よって(9)が示された．

(12)の共役を取り i を $i-1$ とすると $\gamma_{i-1}=-\dfrac{1}{\beta_i'}$ であるから $2\leqq i$ ならば $k_{i-1}=[\gamma_{i-1}]=\left[-\dfrac{1}{\beta_i'}\right]$ となる．(12)と(7)を用いれば

$$\beta_{i-1}=-\frac{1}{\gamma_{i-2}'}=-\gamma_{i-1}'+k_{i-1}$$
$$=\frac{1}{\beta_i}+\left[-\frac{1}{\beta_i'}\right]$$

となる．——

補題 11 $\alpha_n\alpha_n'=\pm 1$ $(1\leqq n)$ とすれば

$$\gamma_0=\gamma_n=\beta_n=\sqrt{m}+[\sqrt{m}].$$

証明 $\alpha_0=1$ であるので $\alpha_0\alpha_0'=1$ である．定理 21 と(9)から γ_0, γ_n, β_n の分母は 1 となり

$$\gamma_0=\sqrt{m}+a_1,\qquad \gamma_n=\sqrt{m}+a_{n+1},\qquad \beta_n=\sqrt{m}+a_n$$

となる．$\gamma_i=\dfrac{\alpha_{i+1}}{\alpha_i}$ から $-\gamma_i'=-\dfrac{{\alpha_{i+1}}'}{{\alpha_i}'}$ となる．$|{\alpha_{i+1}}'|<|{\alpha_i}'|$ であり ${\alpha_{i+1}}'$ と ${\alpha_i}'$ は異符号であるから $0<-\gamma_i'<1$ となる．$\beta_i=-\dfrac{{\alpha_{i-1}}'}{{\alpha_i}'}$ であるから $-\beta_i'=\dfrac{\alpha_{i-1}}{\alpha_i}$ となり $1\leqq i$ ならば $\alpha_{i-1}<\alpha_i$ から $0<-\beta_i'<1$ となる．a を整数とすると $-(\sqrt{m}+a)'=\sqrt{m}-a$ となり $0<\sqrt{m}-a<1$ は $a=[\sqrt{m}]$ を意味する．よって $a_1=a_{n+1}=a_n=[\sqrt{m}]$ となる．——

定理 22 (ガロア, 1828) $\alpha_n\alpha_n'=\pm 1$ $(1\leqq n)$ ならば

$$k_i=k_{n-i}\qquad (1\leqq i\leqq n-1).$$

証明 補題 11 から $\gamma_0=\beta_n$ である．補題 10 の(8)と(10)を使えば $2\leqq n$ ならば $\gamma_1=\beta_{n-1}$ が得られる．同様に(8), (10)を何回も使えば

$$\gamma_i=\beta_{n-i}\qquad (0\leqq i\leqq n-1) \tag{13}$$

が得られる．よって(6)から

$$k_i=[\gamma_i]=[\beta_{n-i}]=k_{n-i}\qquad (1\leqq i\leqq n-1)$$

が得られる．——

(13)から a_i, b_i の対称性が言える．

系 $\alpha_n\alpha_n'=\pm 1$ $(1\leqq n)$ ならば

$$a_{i+1}=a_{n-i},\qquad b_i=b_{n-i}\qquad (0\leqq i\leqq n-1).$$

証明 定理 21 と補題 10 の(9)から

$$\beta_i=\frac{\sqrt{m}+a_i}{b_i},\qquad \gamma_i=\frac{\sqrt{m}+a_{i+1}}{b_i}$$

となる．(12)を使えば求める結果を得る．——

このように k_i, a_i, b_i は対称であることがわかった．では，対称の中心まで計算が進んだことを，どのように判定すればよいのだろうか．また計算を対称の中心まで行なったら中止してよいのだろうか．次の２つの定理がこの疑問に答えてくれる．

定理 23 (Moir, 1874)　b_i $(1\leqq i)$ の中で最初に 1 となるものを b_n とし，$a_i=a_{i+1}$ または $b_i=b_{i+1}$ となる最初の i $(0\leqq i)$ を h とすると

$$a_h = a_{h+1} \Longleftrightarrow n = 2h$$

$$b_h = b_{h+1} \Longleftrightarrow n = 2h+1.$$

証明　定理 21 と (9) から

$$\beta_i = \frac{\sqrt{m}+a_i}{b_i}, \qquad \beta_{i+1} = \frac{\sqrt{m}+a_{i+1}}{b_{i+1}}, \qquad \gamma_i = \frac{\sqrt{m}+a_{i+1}}{b_i}$$

となる．いくつかの場合に分けて証明しよう．

（イ）$a_i=a_{i+1}$ ならば $\beta_i=\gamma_i$ となる．$\beta_0=\sqrt{m}\neq\sqrt{m}+[\sqrt{m}]=\gamma_0$ から $0\neq i$ である．(2) と (7) を書き並べると

$$\beta_{i+1} = \frac{1}{\beta_i-[\beta_i]}, \qquad \gamma_{j-1} = \frac{1}{\gamma_j-[\gamma_j]}$$

となり，よって $\beta_i=\gamma_j$ ならば $\beta_{i+1}=\gamma_{j-1}$ となる．よって $\beta_i=\gamma_i$ から $\beta_{2i}=\gamma_0$ が得られ，γ_0 の分母は 1 であるから $b_{2i}=1$ が得られる．

（ロ）$b_i=b_{i+1}$ ならば $\beta_{i+1}=\gamma_i$ となり（イ）と同様にして $\beta_{2i+1}=\gamma_0$ が得られ，$b_{2i+1}=1$ となる．

（ハ）$a_i=a_{i+1}$ と $b_i=b_{i+1}$ が同時に成立したとする．（イ）から $0<i$ となり，$\beta_{i+1}=\gamma_{i-1}$ となる．（ロ）から $\beta_{i+1}=\gamma_i$ であるから $\gamma_{i-1}=\gamma_i$ となり特に $b_{i-1}=b_i$ となる．

（ニ）$b_{2i}=1$ $(0<i)$ とする．補題 11 から $\gamma_0=\beta_{2i}$ となり，補題 10 の (8) と (10) を並べると

$$\gamma_{i+1} = \frac{1}{\gamma_i}+\left[-\frac{1}{\gamma_i'}\right], \qquad \beta_{i-1} = \frac{1}{\beta_i}+\left[-\frac{1}{\beta_i'}\right]$$

であるから $\gamma_1=\beta_{2i-1}$ となり，同じ操作を繰り返すと $\gamma_i=\beta_i$ となる．これから特に $a_i=a_{i+1}$ が得られる．

(ホ) $b_{2i+1}=1$ とすると(ニ)と同様に $\gamma_0=\beta_{2i+1}$ となり $\gamma_i=\beta_{i+1}$ が成り立ち，$b_i=b_{i+1}$ が得られる．

さて，定理の h および n を定めたとき $a_h=a_{h+1}$ と $b_h=b_{h+1}$ が同時に成立することはない．なぜならばもし $a_h=a_{h+1}$, $b_h=b_{h+1}$ ならば(ハ)から $b_{h-1}=b_h$ となり，h の最小性に反する．

(ヘ) $a_h=a_{h+1}$ ならば(イ)から $b_{2h}=1$ となり $j<2h$ ならば $b_j\neq 1$ である．なぜなら $j=$偶数$=2i<2h$ ならば(ニ)から $a_i=a_{i+1}$ となり h の最小性に反する．$j=$奇数$=2i+1<2h$ ならば(ホ)から $b_i=b_{i+1}$ となりやはり h の最小性に反する．よって $n=2h$ となる．

(ト) 逆に $n=$偶数$=2i$ ならば(ニ)から $a_i=a_{i+1}$ となり $j<i$ に対して $a_j\neq a_{j+1}$, $b_j\neq b_{j+1}$ である．なぜなら $a_j=a_{j+1}$ ならば $b_{2j}=1$ となり $b_j=b_{j+1}$ なら $b_{2j+1}=1$ となり $2j<2j+1<2i$ であるから n の最小性に反する．よって $i=h$ となり $a_h=a_{h+1}$ となる．

(チ) $b_h=b_{h+1}$ のとき，(ロ)から $b_{2h+1}=1$ となり $j<2h+1$ に対しては $b_j\neq 1$ である．なぜなら $j<2h$ に対して $b_j=1$ ならば(ヘ)と同様にして矛盾であり，$b_{2h}=1$ ならば(ニ)から $a_h=a_{h+1}$ となり $a_h=a_{h+1}$ と $b_h=b_{h+1}$ が同時に成り立つことになり矛盾である．よって $n=2h+1$ となる．

(リ) $n=$奇数$=2i+1$ ならば(ホ)から $b_i=b_{i+1}$ となり $j<i$ に対しては(ト)と同様に，$a_j\neq a_{j+1}$, $b_j\neq b_{j+1}$ であるから $i=h$ となり $b_h=b_{h+1}$ となる．

以上で論理的にややこしい証明が終った．——

さて，k_i の対称の中心がわかったので，半分 β_i を計算すればよい．また，次に示すように α_{h+1} まで計算すれば α_n がすぐ計算出来る．

定理 24 $$n=2h \Longrightarrow \alpha_n=\frac{{\alpha_h}^2}{b_h}$$

$$n=2h+1 \Longrightarrow \alpha_n=\frac{\alpha_h\alpha_{h+1}}{b_h}.$$

証明 定理23の証明を利用すると $n=2h$ ならば $\beta_j=\gamma_{n-j}$ が得られ，$\beta_1\beta_2\cdots\beta_h=\gamma_h\gamma_{h+1}\cdots\gamma_{n-1}$ が得られる．定義にもどって書き直せば

$$(-1)^h\frac{\alpha_0'}{\alpha_1'}\frac{\alpha_1'}{\alpha_2'}\cdots\frac{\alpha_{h-1}'}{\alpha_h'}=\frac{\alpha_{h+1}}{\alpha_h}\frac{\alpha_{h+2}}{\alpha_{h+1}}\cdots\frac{\alpha_n}{\alpha_{n-1}}.$$

よって $(-1)^h\dfrac{1}{\alpha_h'}=\dfrac{\alpha_n}{\alpha_h}$ となる．よって

$$\alpha_n=(-1)^h\frac{\alpha_h}{\alpha_h'}=\frac{\alpha_h^2}{(-1)^h\alpha_h\alpha_h'}$$

$$=\frac{\alpha_h^2}{b_h}.$$

次に $n=2h+1$ とする．$h=0$ ならば $\alpha_0=1$，$b_0=1$ であるから $\alpha_1=\dfrac{\alpha_0\alpha_1}{b_0}$ となる．$h\geqq 1$ ならば $\beta_i=\gamma_{n-i}$ から $\beta_1\beta_2\cdots\beta_h=\gamma_{h+1}\gamma_{h+2}\cdots\gamma_{n-1}$ が得られ

$$(-1)^h\frac{\alpha_0'}{\alpha_1'}\frac{\alpha_1'}{\alpha_2'}\cdots\frac{\alpha_{h-1}'}{\alpha_h'}=\frac{\alpha_{h+2}}{\alpha_{h+1}}\frac{\alpha_{h+3}}{\alpha_{h+2}}\cdots\frac{\alpha_n}{\alpha_{n-1}}$$

から $(-1)^h\dfrac{1}{\alpha_h'}=\dfrac{\alpha_n}{\alpha_{h+1}}$ が得られる．よって

$$\alpha_n=(-1)^h\frac{\alpha_{h+1}}{\alpha_h'}=\frac{\alpha_h\alpha_{h+1}}{(-1)^h\alpha_h\alpha_h'}$$

$$=\frac{\alpha_h\alpha_{h+1}}{b_h}$$

となる．——

たとえば $m=19$ のとき $a_3=a_4$ となるので $n=6$ となり $\alpha_{-1}=\sqrt{19}$，$\alpha_0=1$，$\alpha_1=4+\sqrt{19}$，$\alpha_2=9+2\sqrt{19}$，$\alpha_3=13+3\sqrt{19}$ から

$$\frac{\alpha_3^2}{b_3}=\frac{(13+3\sqrt{19})^2}{2}$$

$$=\frac{169+2\cdot 13\cdot 3\sqrt{19}+171}{2}$$

$$= 170+39\sqrt{19} = \alpha_6$$

となる．$m=61$ のときは $b_5=b_6$ となるので $n=11$ となり $\alpha_{-1}=\sqrt{61}$, $\alpha_0=1$, $\alpha_1=7+\sqrt{61}$, $\alpha_2=8+\sqrt{61}$, $\alpha_3=39+5\sqrt{61}$, $\alpha_4=125+16\sqrt{61}$, $\alpha_5=164+21\sqrt{61}$, $\alpha_6=453+58\sqrt{61}$ となり

$$\frac{\alpha_5\alpha_6}{b_5} = \frac{(164+21\sqrt{61})(453+58\sqrt{61})}{5}$$
$$= 29718+3805\sqrt{61} = \alpha_{11}$$

となる．

§7 ラグランジュの定理

$\beta_1, \beta_2, \cdots$ と計算していくと，必ず分母が1になるものが現われるだろうか．ラグランジュは**部屋割り論法**を用い，ペル方程式は必ず解を持つことを示した．

補題 12 $\beta_i = \dfrac{\sqrt{m}+a_i}{b_i}$ とすると

$$0 \leqq a_i < \sqrt{m}, \qquad 0 < b_i < 2\sqrt{m}.$$

証明 $|\alpha_{i-1}'|>|\alpha_i'|$ から

$$1 < -\frac{\alpha_{i-1}'}{\alpha_i'} = \beta_i = \frac{\sqrt{m}+a_i}{b_i}$$

である．両辺に -1 を掛け，共役を取ると $\dfrac{\alpha_{i-1}}{\alpha_i}=\dfrac{\sqrt{m}-a_i}{b_i}$ となる．$i=0$ ならば $\beta_0=\sqrt{m}$ であるから $a_0=0$, $b_0=1$ となり補題は成り立つ．$i>0$ のとき $0<\dfrac{\alpha_{i-1}}{\alpha_i}<1<\beta_i$ であるから

$$0 < \frac{\sqrt{m}-a_i}{b_i} < 1 < \frac{\sqrt{m}+a_i}{b_i}$$

となる．$b_i=|\alpha_i\alpha_i'|$ であるから $b_i>0$ となり，よって $\dfrac{\sqrt{m}-a_i}{b_i} < \dfrac{\sqrt{m}+a_i}{b_i}$ から $0<a_i$ となる．また $0<\dfrac{\sqrt{m}-a_i}{b_i}$ から $a<\sqrt{m}$ が得られる．よって $1<\dfrac{\sqrt{m}+a_i}{b_i}$ から $b_i<\sqrt{m}+a_i<\sqrt{m}+\sqrt{m} = 2\sqrt{m}$

となり補題の証明は終った. ——

定理 25 (ラグランジュ, 1766-1767ごろ) $\alpha_n\alpha_n'=\pm1$ となる自然数 n が存在する.

証明 $\gamma_i=\dfrac{\sqrt{m}+a_{i+1}}{b_i}$ であるが, 補題12から a_{i+1}, b_i の範囲はかぎられている. これらは整数であるから a_{i+1} は $0, 1, \cdots, [\sqrt{m}]$ の $[\sqrt{m}]+1$ 通りしかなく, b_i は $1, 2, \cdots, [2\sqrt{m}]$ の $[2\sqrt{m}]$ 通りしかない. よって a_{i+1} と b_i の組合せは多くとも $c=([\sqrt{m}]+1)[2\sqrt{m}]$ 通りしかなく有限である. よって γ_i の取り得る値は多くとも c 通りである. よって $\gamma_0, \gamma_1, \cdots, \gamma_c$ の中には同じ値のものがある(部屋割り論法). $i<n$ で $\gamma_i=\gamma_n$ となる最小の i は0である. なぜならば $0<i$ のとき, 前節の(7)から $\gamma_{i-1}=\gamma_{n-1}$ となり i の最小性に反するからである. $\gamma_0=\gamma_n$ ということは $|\alpha_n\alpha_n'|=b_n=1$ を意味する. ——

さて, この定理から $\alpha\cdot\alpha'=\pm1$ となる解が $\alpha=1$ 以外に1つはあることがわかった. このペル方程式の最小の解を α_n とすると $\alpha_n{}^q(\alpha_n{}^q)'=\alpha_n{}^q(\alpha_n')^q=(\alpha_n\alpha_n')^q=(\pm1)^q$ から $\alpha_n{}^q$ (q=自然数)も解である. しかし $\alpha_n{}^q$ 以外には解がないことを示そう.

定理 26 ペル方程式の最小の解を α_n とおけばすべての解は

$$\alpha_{nq}=\alpha_n{}^q \qquad (q=1, 2, \cdots)$$

となる.

証明 ペル方程式 $\alpha\alpha'=\pm1$ の解は $\alpha_1, \alpha_2, \cdots$ の数列の中にあることは§4(2)で説明した.

さて $\alpha_n\alpha_n'=\pm1$ であるから補題11から $\gamma_0=\gamma_n$ となる. よって補題10の(8)から $\gamma_1=\gamma_{n+1}, \gamma_2=\gamma_{n+2}, \cdots$ となり $\gamma_i=\gamma_{n+i}$ となる. i の代りに $n+i$ とおけば $\gamma_{n+i}=\gamma_{n+n+i}=\gamma_{2n+i}$ となり同様に続けると

$$\gamma_i=\gamma_{n+i}=\gamma_{2n+i}=\cdots$$

となる.

ところで $\alpha_l\alpha_l'=\pm 1$ となったとする．$l=n\cdot q+r$ $(0\leqq r<n)$ とおけば $\gamma_r=\gamma_{nq+r}=\gamma_l$ となる．補題11から $\gamma_l=\gamma_0$ となるので $\gamma_0=\gamma_r$ となり $b_r=1$ となる．これは n の最小性から $r=0$ を意味する．よって $l=n\cdot q$ となる．このとき

$$\alpha_l=\frac{\alpha_1}{\alpha_0}\frac{\alpha_2}{\alpha_1}\cdots\frac{\alpha_l}{\alpha_{l-1}}=\gamma_0\gamma_1\cdots\gamma_{l-1}$$

$$=\gamma_0\gamma_1\cdots\gamma_{n-1}\gamma_n\gamma_{n+1}\cdots\gamma_{n+n-1}\cdots\gamma_{l-1}.$$

$\gamma_i=\gamma_{n+i}$ であるから

$$=(\gamma_0\gamma_1\cdots\gamma_{n-1})(\gamma_0\gamma_1\cdots\gamma_{n-1})\cdots(\gamma_0\gamma_1\cdots\gamma_{n-1})$$

$$=\left(\frac{\alpha_1}{\alpha_0}\cdots\frac{\alpha_n}{\alpha_{n-1}}\right)^q=\alpha_n{}^q$$

となる．——

§8 アルゴリズム(計算法)

さて，m が与えられたとき，いかに能率的に $\alpha_n\alpha_n'=\pm 1$ となる最小の α_n を求めるか，考えてみよう．第4章§7の例をふたたび書くと

補題 13 α を実数，n を自然数とすると

(1) $$[\alpha+n]=[\alpha]+n$$

(2) $$\left[\frac{\alpha}{n}\right]=\left[\frac{[\alpha]}{n}\right].$$ ——

この補題により

$$k_i=[\beta_i]=\left[\frac{\sqrt{m}+a_i}{b_i}\right]=\left[\frac{[\sqrt{m}+a_i]}{b_i}\right]=\left[\frac{[\sqrt{m}]+a_i}{b_i}\right]$$

となる．$\beta_0=\sqrt{m}$ から $k_0=[\sqrt{m}]$ となり

(3) $$k_i=\left[\frac{k_0+a_i}{b_i}\right]$$

となる．よって $\sqrt{m}$ の小数部を計算する必要はない．k_i が計算出

来たとき

$$\beta_{i+1}=\frac{1}{\beta_i-k_i}$$
$$=\frac{1}{(\sqrt{m}+a_i)/b_i-k_i}$$
$$=\frac{1}{(\sqrt{m}+a_i-k_ib_i)/b_i}$$
$$=\frac{\sqrt{m}-a_i+k_ib_i}{(\sqrt{m}+a_i-k_ib_i)(\sqrt{m}-a_i+k_ib_i)/b_i}$$
$$=\frac{\sqrt{m}+a_{i+1}}{b_{i+1}}$$

となる．よって

(4) $$a_{i+1}=k_ib_i-a_i$$

(5) $$b_{i+1}=\frac{m-{a_{i+1}}^2}{b_i}.$$

i を $i-1$ に変えれば

$$b_i=\frac{m-{a_i}^2}{b_{i-1}}$$

(6) $$\therefore\quad b_{i-1}=\frac{m-{a_i}^2}{b_i}$$

となる．この式を使えば

$$b_{i+1}=\frac{m-(k_ib_i-a_i)^2}{b_i}$$
$$=\frac{m-{k_i}^2{b_i}^2+2k_ib_ia_i-{a_i}^2}{b_i}$$
$$=\frac{m-{a_i}^2}{b_i}+k_i(2a_i-k_ib_i).$$

(4) と (6) を使えば

(7) $$b_{i+1}=b_{i-1}+k_i(a_i-a_{i+1}).$$

このように β_i は次々に計算されていく．次に α_i を考えよう．$\alpha_i=p_i+q_i\sqrt{m}$ とおくと $\alpha_{-1}=\sqrt{m}$, $\alpha_0=1$ であるから $p_{-1}=0$, $p_0=1$, $q_{-1}=1$, $q_0=0$ が得られる．

$$\begin{aligned}\alpha_{i+1} &= \alpha_{i-1}+k_i\alpha_i\\ &= (p_{i-1}+q_{i-1}\sqrt{m})+k_i(p_i+q_i\sqrt{m})\\ &= (p_{i-1}+k_ip_i)+(q_{i-1}+k_iq_i)\sqrt{m}\end{aligned}$$

であるから

(8) $$p_{i+1}=p_{i-1}+k_ip_i$$

(9) $$q_{i+1}=q_{i-1}+k_iq_i$$

と計算出来る．また p_i は q_i から次のように計算出来る．

$$\frac{\sqrt{m}+a_i}{b_i}=\beta_i=-\frac{\alpha_{i-1}'}{\alpha_i'}=-\frac{p_{i-1}-q_{i-1}\sqrt{m}}{p_i-q_i\sqrt{m}}$$

$$\begin{aligned}b_i(-p_{i-1}+q_{i-1}\sqrt{m}) &= (p_i-q_i\sqrt{m})(\sqrt{m}+a_i)\\ &= (p_ia_i-q_im)+(p_i-q_ia_i)\sqrt{m}.\end{aligned}$$

$\sqrt{m}$ の係数を比べると

$$b_iq_{i-1}=p_i-q_ia_i.$$

(10) $$\therefore\quad p_i=a_iq_i+b_iq_{i-1}$$

となる．

まとめると $\beta_0=\sqrt{m}$ から $a_0=0$, $b_0=1$ となり $k_0=[\sqrt{m}]$ となる．次に(4), (5), (3)から a_1, b_1, k_1 が得られる．これ以後は(4), (7), (3)から a_i, b_i, k_i が得られる．$a_i=a_{i+1}$ または $b_i=b_{i+1}$ となったとき，計算を中止すればよい．次に α_i については $q_{-1}=1$, $q_0=0$ と(9)から q_i が計算出来，p_i は(10)を使えば計算量が少なくてすむ．たとえば $m=19$ のとき，$[\sqrt{m}]=4$ となり

$$\beta_0=\sqrt{19},\qquad a_0=0,\qquad b_0=1,\qquad k_0=4,$$

$$a_1=k_0b_0-a_0=4,\qquad b_1=\frac{m-a_1^2}{b_0}=3$$

$$k_1 = \left[\frac{k_0+a_1}{b_1}\right] = \left[\frac{4+4}{3}\right] = 2$$

$$a_2 = k_1b_1-a_1 = 2, \qquad b_2 = b_0+k_1(a_1-a_2) = 5$$

$$k_2 = \left[\frac{k_0+a_2}{b_2}\right] = \left[\frac{4+2}{5}\right] = 1$$

$$a_3 = k_2b_2-a_2 = 3, \qquad b_3 = b_1+k_2(a_2-a_3) = 2$$

$$k_3 = \left[\frac{k_0+a_3}{b_3}\right] = \left[\frac{4+3}{2}\right] = 3$$

$$a_4 = k_3b_3-a_3 = 3$$

ここで $a_3=a_4$ であるから $n=6$ となる．$q_{-1}=1$，$q_0=0$ であるから

$$q_1 = q_{-1}+k_0q_0 = 1$$

$$q_2 = q_0+k_1q_1 = 2$$

$$q_3 = q_1+k_2q_2 = 3$$

$$p_3 = a_3q_3+b_3q_2 = 9+4 = 13.$$

よって $\alpha_3=13+3\sqrt{19}$ となり $\alpha_6=\dfrac{{\alpha_3}^2}{b_3}=170+39\sqrt{19}$ が得られるわけである．

第9章　素数判定法

§1　Pepin の判定法

フェルマー数とは

$$F_n = 2^{2^n}+1$$

という形をした素数である．このことはすでに学んだ．F_0, F_1, F_2, F_3, F_4 は素数であることが知られているが，$n \geqq 5$ のときは1つも素数である F_n が見つかっていない．以後 $n \geqq 1$ として，F_n が素数か否かをどのように判定するかを述べよう．

まず F_n に素因子 p があるとしたら

$$p \mid F_n \Longrightarrow p \equiv 1 \pmod{2^{n+1}}$$

であることを示そう．F_n の定義により

$$\begin{aligned} p \mid F_n &\Longrightarrow 2^{2^n}+1 \equiv 0 \pmod{p} \\ &\Longrightarrow 2^{2^n} \equiv -1 \pmod{p} \\ &\Longrightarrow (2^{2^n})^2 \equiv 1 \pmod{p} \\ &\Longrightarrow 2^{2^{n+1}} \equiv 1 \pmod{p} \end{aligned}$$

となる．2を 2^{n+1} 乗すると1と合同になるのだから，2の $\mathrm{mod}\, p$ での位数は 2^{n+1} の約数である．ところが 2^{n+1} の約数は

$$1,\ 2,\ 2^2,\ 2^3,\ \cdots,\ 2^n,\ 2^{n+1}$$

しかない．もし位数が 2^k $(k \leqq n)$ ならば，$2^k \mid 2^n$ であるから2を 2^n 乗すれば，$\mathrm{mod}\, p$ で1と合同になるはずである．ところが $2^{2^n} \equiv -1$ であるから矛盾となり，2の $\mathrm{mod}\, p$ での位数は 2^{n+1} となる．位数は $\varphi(p) = p-1$ の約数であるから

$$p-1 \equiv 0 \pmod{2^{n+1}}$$

$$\therefore\quad p \equiv 1 \pmod{2^{n+1}}$$

が得られた.

オイラー(1732)はF_5が合成数であることを示すために，$p\equiv 1 \pmod{64}$という形をした素数で小さい順にF_5を割っていき

$$F_5 = 2^{32}+1 = 4294967297$$
$$= 641\times 6700417$$

であることを見つけた. $641=1+64\times 10$である.

ランドリー(1880)はF_6の素因子も$p\equiv 1 \pmod{128}$の中から見つけた. その結果は

$$F_6 = 18446744073709551617$$
$$= 274177\times 67280421310721$$
$$274177 = 2142\times 128+1$$

である. これは手計算なので，いかに大変な計算か想像つくであろう.

ところで，素数か否かだけの判定ならば，次のようにして出来る.

$$F_n = \text{素数} \Longleftrightarrow 3^{(F_n-1)/2} \equiv -1 \pmod{F_n}.$$

これを**Pepinの判定法**という. これを証明してみよう.

まず，F_n=素数 とする.

$$F_n = 2^{2^n}+1$$
$$\equiv (-1)^{2^n}+1 \pmod 3$$
$$= 2 \qquad (\because\ n\geqq 1)$$

であるから$(F_n, 3)=1$である. よってフェルマーの定理から

$$3^{F_n-1} \equiv 1 \pmod{F_n}$$

であり，$F_n-1=2^{2^n}$は偶数であるから

$$(3^{(F_n-1)/2}-1)(3^{(F_n-1)/2}+1) \equiv 0 \pmod{F_n}$$

となり$3^{(F_n-1)/2}$は1または-1と$\mathrm{mod}\ F_n$で合同である. もし

$$3^{(F_n-1)/2} \equiv 1 \pmod{F_n}$$

ならば，オイラーの規準によりルジャンドル記号が

$$(1) \qquad \left(\frac{3}{F_n}\right) = 1$$

となる．ところで $n \geqq 1$ から

$$F_n = 2^{2^n} + 1 \equiv 1 \pmod 4$$

であるから，相互律により

$$\begin{aligned} \left(\frac{3}{F_n}\right) &= \left(\frac{F_n}{3}\right) \\ &= \left(\frac{2}{3}\right) \qquad \because \quad F_n \equiv 2 \pmod 3 \\ &= -1 \end{aligned}$$

となり(1)と矛盾する．よって

$$(2) \qquad 3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$$

が得られた．

逆に(2)が成り立っているとすると，両辺を自乗して

$$3^{F_n-1} \equiv 1 \pmod{F_n}$$

となる．よって mod F_n に関しての 3 の位数は F_n-1 の約数である．$F_n-1=2^{2^n}$ であるから，その約数は

$$1,\ 2,\ 2^2,\ \cdots,\ 2^{2^n-1} = \frac{F_n-1}{2},\ 2^{2^n}$$

となる．よって(2)から位数が 2^{2^n} であることがわかった．位数は $\varphi(F_n)$ の約数であるので

$$2^{2^n} \leqq \varphi(F_n) \leqq F_n - 1 = 2^{2^n}$$

から $\varphi(F_n)=F_n-1$ が得られる．この式は 1 から F_n までの中で，F_n と互いに素な数の個数が F_n-1 個あることを意味する．つまり 1, 2, …, F_n-1 は F_n と素となり，F_n は素数となる．

例　$n=3$ のとき

$$F_3 = 2^{2^3}+1 = 2^8+1 = 257$$

$$3^2 = 9$$

$$3^{2^2} = 81$$
$$3^{2^3} = 81^2 \equiv 136 \pmod{257}$$
$$3^{2^4} \equiv 136^2 \equiv 249 \pmod{257}$$
$$3^{2^5} \equiv 249^2 \equiv 64 \pmod{257}$$
$$3^{2^6} \equiv 64^2 \equiv 241 \pmod{257}$$
$$3^{2^7} \equiv 241^2 \equiv -1 \pmod{257}.$$

よって F_3 は素数である．——

§2 ルカステスト

メルセンヌ数とは

$$M_p \equiv 2^p-1 \qquad (p=\text{素数})$$

という形をした素数である．第3章§5で述べたが今までに27個見つかっている．次に M_p が素数か否かの判定法を述べよう．以後 p は3以上の素数としよう．

まず，M_p に素因子 q があったとすると，M_p は奇数であるから，q も奇数となり

(1) $$2^p \equiv 1 \pmod{q}$$

となる．よって，2の $\bmod q$ での位数は p の約数になるが，p の約数には1と p しかない．$2 \not\equiv 1 \pmod{q}$ であるから，2の位数は p となる．位数は $\varphi(q)=q-1$ の約数であるから

$$q \equiv 1 \pmod{p}$$

が得られた．よって $q=k\cdot p+1$ という形であるが，k が奇数だと p も奇数だから，q は偶数になってしまう．よって $q=2k'p+1$ という形をしている．

例 $M_{11} = 2^{11}-1 = 2047 = 23\times 89$

$23 = 2\times 11+1, \qquad 89 = 8\times 11+1.$ ——

例 $M_{23} = 2^{23}-1 = 8388607 = 47\times 178481$

$$47 = 2\times 23+1, \qquad 178481 = 7760\times 23+1. \text{ ——}$$

ところで(1)が成り立つとき，両辺を2倍すれば

$$2 \equiv 2^{p+1} = (2^{(p+1)/2})^2 \pmod q$$

となる．よって，2は mod q で平方剰余となっている．よって第2補充法則から

$$q \equiv 1 \quad \text{または} \quad q \equiv -1 \pmod 8$$

となる．

例
$$M_{11} = 23\times 89$$
$$23 = 3\times 8-1, \qquad 89 = 11\times 8+1. \text{ ——}$$

例
$$M_{23} = 47\times 178481$$
$$47 = 6\times 8-1, \qquad 178481 = 22310\times 8+1. \text{ ——}$$

M_p について，次のようなことも言える(オイラー)．

$$p \equiv 3 \pmod 4, \qquad 2p+1 = \text{素数} \Longrightarrow 2p+1\,|\,M_p$$

($a|b$ は a が b の約数であることを意味する．) なぜならば $q=2p+1$ とおけば $p=4k+3$ と書けるので

$$q = 2(4k+3)+1 \equiv -1 \pmod 8$$

となり，よって $\left(\dfrac{2}{q}\right)=1$ となる．このとき，オイラー規準により

$$\begin{aligned} 1 &= \left(\frac{2}{q}\right) \\ &\equiv 2^{(q-1)/2} \pmod q \\ &= 2^p \end{aligned}$$

であるから $M_p=2^p-1$ が q で割れる．特に $p>3$ ならば

$$M_p = 2^p-1 > 2p+1 = q$$

であるから M_p は素数でない．

例　$23|M_{11}$,　$47|M_{23}$,　$167|M_{83}$,　$263|M_{131}$,
$359|M_{179}$,　$383|M_{191}$,　$479|M_{239}$,　$503|M_{251}$,
$719|M_{359}$,　$839|M_{419}$. ——

以上のように M_p の素因子がわかることもあるが，素因子がわからなくとも，素数か合成数かの判定は出来る．それは次のような**ルカステスト**があるからである．

p を奇素数とし

$$S_1 = 4$$
$$S_2 = S_1{}^2 - 2$$
$$S_3 = S_2{}^2 - 2$$
$$\cdots$$

と S_i を次々に定めていくと

$$M_p = 2^p - 1 = \text{素数} \Longleftrightarrow M_p | S_{p-1}$$

となる(ルカス，1876)．

例 $p=7$ のとき $M_7=2^7-1=127$.

$$S_1 = 4$$
$$S_2 = 16-2 = 14$$
$$S_3 = 14^2-2 \equiv 67 \pmod{127}$$
$$S_4 \equiv 67^2-2 \equiv 42 \pmod{127}$$
$$S_5 \equiv 42^2-2 = 111 \pmod{127}$$
$$S_6 \equiv 111^2-2 \equiv 0 \pmod{127}.$$

よって，M_7 は素数である．——

つぎに長くなるが，D. H. レーマー(1934)の証明を少し改良して述べよう．

まず，ペル方程式

(2) $$x^2-3y^2 = 1$$

を考えよう．3は平方数ではないので，無限に自然数解があり最小の解は $x_1=2, y_1=1$ となり，n 番目の解 x_n, y_n は

(3) $$(2+\sqrt{3})^n = x_n+\sqrt{3}\,y_n$$

から得られる．2項定理で展開すると

$$(2+\sqrt{3})^n = \sum_{i=0}^{n}\binom{n}{i}2^{n-i}(\sqrt{3})^i$$
$$= \sum_k \binom{n}{2k}2^{n-2k}3^k + \sum_k \binom{n}{2k+1}2^{n-2k-1}3^k\sqrt{3}$$

となるので

(4) $$x_n = \sum_k \binom{n}{2k}2^{n-2k}3^k, \qquad y_n = \sum_k \binom{n}{2k+1}2^{n-2k-1}3^k$$

が得られる．$(2+\sqrt{3})^n$ の共役は $(2-\sqrt{3})^n$ であるから

(5) $$x_n = \frac{1}{2}\{(x_n+\sqrt{3}\,y_n)+(x_n-\sqrt{3}\,y_n)\}$$
$$= \frac{1}{2}\{(2+\sqrt{3})^n+(2-\sqrt{3})^n\}$$

(6) $$y_n = \frac{1}{2\sqrt{3}}\{(x_n+\sqrt{3}\,y_n)-(x_n-\sqrt{3}\,y_n)\}$$
$$= \frac{1}{2\sqrt{3}}\{(2+\sqrt{3})^n-(2-\sqrt{3})^n\}$$

となる．また

$$(x_m+\sqrt{3}\,y_m)(x_m-\sqrt{3}\,y_m)$$
$$= x_m{}^2-3y_m{}^2 = 1$$

であるから

$$(x_m+\sqrt{3}\,y_m)^{-1} = (x_m-\sqrt{3}\,y_m)$$

となり

$$(2+\sqrt{3})^{n\pm m} = (2+\sqrt{3})^n(2+\sqrt{3})^{\pm m}$$
$$= (x_n+\sqrt{3}\,y_n)(x_m\pm\sqrt{3}\,y_m)$$
$$= (x_nx_m\pm 3y_ny_m)+\sqrt{3}(\pm x_ny_m+x_my_n)$$

から

(7) $$x_{n\pm m} = x_nx_m\pm 3y_ny_m$$

(8) $$y_{n\pm m} = \pm x_ny_m+x_my_n$$

が得られる．(8)において $m=1$ とおくと

(9) $$y_{n-1} = -x_n + 2y_n$$

となる．$n=m$ とおけば，(2) から倍角公式

(10) $$x_{2n} = x_n{}^2 + 3y_n{}^2 = x_n{}^2 + (x_n{}^2 - 1) = 2x_n{}^2 - 1$$

(11) $$y_{2n} = 2x_n y_n$$

が得られる．この公式から

$$S_i = 2x_{2^{i-1}}$$

が得られる．なぜならば，まず $i=1$ のとき

$$S_1 = 4, \qquad 2x_{2^{i-1}} = 2x_1 = 2\cdot 2 = 4$$

となり成立する．$i=k$ まで成り立つとすると

$$\begin{aligned} S_{k+1} = S_k{}^2 - 2 &= (2x_{2^{k-1}})^2 - 2 \\ &= 2(2x_{2^{k-1}}{}^2 - 1) \\ &= 2x_{2\cdot 2^{k-1}} \\ &= 2x_{2^k} \end{aligned}$$

となり $i=k+1$ のときも成立する．このことからルカステストは M_p＝奇数 から

(12) $$M_p = \text{素数} \Longleftrightarrow M_p \mid x_{2^{p-2}}$$

と同じになる．以後この命題を証明しよう．そのために，q が 3 より大きな素数のとき

(13) $$y_{(q+1)/2}\, y_{(q-1)/2} \equiv 0 \pmod q$$

を示そう．$t=(q+1)/2$ とおき

$$2+\sqrt{3} = \frac{(1+\sqrt{3})^2}{2}, \qquad 2-\sqrt{3} = \frac{(1-\sqrt{3})^2}{2}$$

を利用すると，(5) から

$$x_t = \frac{1}{2}\left\{\frac{1}{2^t}(1+\sqrt{3})^{q+1} + \frac{1}{2^t}(1-\sqrt{3})^{q+1}\right\}$$

$$= \frac{1}{2^t}\sum_k \binom{q+1}{2k} 3^k$$

となる．ところで $2k \neq 0$, $2k \neq q+1$ のとき

$$\binom{q+1}{2k} = \binom{q}{2k} + \binom{q}{2k-1}$$

となり $0<2k<q$, $0<2k-1<q$ であるから，右辺は共に q で割り切れる．なぜならば一般に $0<m<q$, q=素数 ならば

$$\binom{q}{m} = \frac{q(q-1)\cdots(q-m+1)}{1\cdot 2\cdot\cdots\cdot m}$$

の分子は q で割れ，分母は q で割れないから $\binom{q}{m}$ は q で割り切れる．よって

$$(14) \qquad 2^t x_t = \sum_k \binom{q+1}{2k} 3^k \equiv 1+3^t \pmod q$$

となる．同様に(6)から y_t を計算すると

$$y_t = \frac{1}{2\sqrt{3}}\left\{\frac{1}{2^t}(1+\sqrt{3})^{q+1} - \frac{1}{2^t}(1-\sqrt{3})^{q+1}\right\}$$

$$= \frac{1}{2^t}\sum_k \binom{q+1}{2k+1} 3^k$$

となり，$2k+1 \neq 1$, $2k+1 \neq q$ のとき

$$\binom{q+1}{2k+1} = \binom{q}{2k+1} + \binom{q}{2k}$$

となり，$0<2k+1<q$, $0<2k<q$ であるから

$$(15) \quad 2^t y_t = \sum_k \binom{q+1}{2k+1} 3^k \equiv \binom{q+1}{1} + \binom{q+1}{q} 3^{t-1} \pmod q$$

$$\equiv 1+3^{t-1} \pmod q$$

となる．よって(9), (14), (15)から

$$\begin{aligned} 2^t y_t \cdot 2^t \cdot y_{t-1} &\equiv (1+3^{t-1})\cdot 2^t \cdot (-x_t+2y_t) \\ &\equiv (1+3^{t-1})(-1-3^t+2+2\cdot 3^{t-1}) \\ &= (1+3^{t-1})(1-3^{t-1}) \end{aligned}$$

$$= 1-3^{2(t-1)}$$
$$= 1-3^{q-1}$$
$$\equiv 0 \pmod{q}.$$

よって(13)が示された.

さて $y_n\equiv 0 \pmod{q}$ となる最小の自然数 n を w としよう. (13)は

(16) $$2w \leqq q+1$$

を示している. 次に w の性質として

(17) $$y_n \equiv 0 \pmod{q} \Longleftrightarrow w|n$$

を示そう. $n=kw$ ならば

$$y_{kw} = y_{(k-1)w+w} = x_{(k-1)w}\cdot y_w + x_w\cdot y_{(k-1)w}$$

から帰納法を使えば $y_n\equiv 0 \pmod{q}$ が得られる. 逆に $y_n\equiv 0 \pmod{q}$ ならば

$$y_{n-kw} = -x_n y_{kw} + x_{kw} y_n \equiv 0 \pmod{q}$$

となる. $n=kw+r$, $0<r<w$ ならば $y_r\equiv 0 \pmod{q}$ となり, w の最小性に反する. よって $r=0$ となり(17)が示された.

以上の準備をし(12)を示そう. まず $x_{2^{p-2}}$ が M_p で割れたとする. q を M_p の素因子とすれば, p が奇数なので $M_p=2^p-1\equiv 2-1=1 \pmod{3}$ から $q>3$ となり, (11)から

$$y_{2^{p-1}} = 2x_{2^{p-2}}y_{2^{p-2}} \equiv 0 \pmod{q}$$

となる. (2)から $(x_n, y_n)=1$ であるから $y_{2^{p-2}}\not\equiv 0 \pmod{q}$ である. よって $w=2^{p-1}$ となる. よって(16)から

$$q+1 \geqq 2w = 2^p = M_p+1 \geqq q+1$$

となり $M_p=q$, つまり $M_p=$素数 となる.

逆に $M_p=q=$素数 とすると $q=2^p-1\equiv -1 \pmod{8}$ であるから, オイラー規準により

$$2^{(q-1)/2} \equiv 1 \pmod{q}$$

となり, $q\equiv -1 \pmod{4}$, $q\equiv 1 \pmod{3}$ から

$$\left(\frac{3}{q}\right) = -\left(\frac{q}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

$$\therefore \quad 3^{(q-1)/2} \equiv -1 \pmod{q}$$

となる．よって $2^{p-1} = \dfrac{q+1}{2} = \dfrac{q-1}{2} + 1$ と(14)から

$$2x_{2^{p-1}} \equiv 1-3 = -2 \pmod{q}$$

となり $x_{2^{p-1}} \equiv -1 \pmod{q}$ が得られた．他方，倍角公式から $x_{2^{p-1}} = 2x_{2^{p-2}} - 1$ となるので $x_{2^{p-2}} \equiv 0 \pmod{q}$ となる．つまり M_p が $x_{2^{p-2}}$ の約数となり証明が完成した．

§3　フェルマーテストの拡張

もし，N＝素数 ならば$(a, N)=1$ となる a に対して

(1) $$a^{N-1} \equiv 1 \pmod{N}$$

となる．よって，もし(1)が成立しなければ，N は合成数となる．これをフェルマーテストという．ただし(1)が成立しても，N＝素数，と判定出来ない．しかし，$N-1$ が素因子分解されていて

$$N-1 = p_1^{f_1} \cdot p_2^{f_2} \cdot \cdots \cdot p_r^{f_r}$$

となるならば，次の判定法で多くの場合，N＝素数，であることがわかる．その判定法とは，$1 \leqq k \leqq r$ となる k に対してそれぞれ

(2) $$(a_k, N) = 1$$

(3) $$a_k^{N-1} \equiv 1 \pmod{N}$$

(4) $$a_k^{(N-1)/p_k} \not\equiv 1 \pmod{N}$$

となる a_k が見つかれば，N＝素数，と判定出来る．（$a_1, a_2, \cdots, a_r$ は同じものがあってもよいし，異なってもかまわない．）なぜならば，$\bmod N$ での a_k の位数 e_k を考えると(3)から e_k は $N-1$ の約数である．よって

$$e_k = p_1^{g_1} \cdot p_2^{g_2} \cdot \cdots \cdot p_r^{g_r}, \qquad g_i \leqq f_i,\ 1 \leqq i \leqq r$$

と書ける．もし $g_k \leqq f_k - 1$ ならば

$$p_1^{g_1}\cdot p_2^{g_2}\cdot\cdots\cdot p_k^{g_k}\cdot\cdots\cdot p_r^{g_r}\,|\,p_1^{f_1}\cdot p_2^{f_2}\cdot\cdots\cdot p_k^{f_k-1}\cdot\cdots\cdot p_r^{f_r}=(N-1)/p_k$$

となり，(4)に反する．よってe_kは$p_k^{f_k}$で割れる．位数は$\varphi(N)$の約数であるから$p_k^{f_k}$は$\varphi(N)$の約数である．このことがkを1からrまで動かしたとき成立するので，$\varphi(N)$は$p_k^{f_k}$の積，つまり$p_1^{f_1}\cdot p_2^{f_2}\cdot\cdots\cdot p_r^{f_r}=N-1$で割れて

$$N-1\leqq\varphi(N)$$

となる．$\varphi(N)$は$1, 2, \cdots, N$までの中でNと素な数の個数であるから，最も大きくなったとしても$N-1$である．よって$N-1=\varphi(N)$となり，これは$1, 2, \cdots, N-1$がNと素であること，つまりNが素数であることを表わす．

例 $N=251$のとき$N-1=250=2\times 5^3$．$N-1, (N-1)/2, (N-1)/5$を2進法で表わすと11111010, 1111101, 110010となるので，mod 251で計算すると，次のようになる．

$$\begin{aligned}
2^7 &= 128\\
2^{15} &= 128^2\cdot 2\equiv 138\\
2^{31} &\equiv 138^2\cdot 2\equiv 187\\
2^{62} &\equiv 187^2\equiv 80\\
2^{125} &\equiv 80^2\cdot 2\equiv -1\not\equiv 1\\
2^{250} &\equiv (-1)^2=1.
\end{aligned}$$

よって$p_1=2$に対しては$a_1=2$とおくと，(2), (3), (4)が成り立つ．$p_2=5$に対しては$a_2=3$とおくと，

$$\begin{aligned}
3^3 &= 27\\
3^6 &= 27^2\equiv 227\\
3^{12} &\equiv 227^2\equiv 74\\
3^{25} &\equiv 74^2\cdot 3\equiv 113\\
3^{50} &\equiv 113^2\equiv 219\not\equiv 1\\
3^{100} &\equiv 219^2\equiv 20
\end{aligned}$$

$$3^{200} \equiv 20^2 \equiv 149$$

$$3^{250} = 3^{200}\cdot 3^{50} \equiv 149\cdot 219 \equiv 1$$

となり，やはり(2)，(3)，(4)が成り立ち，$N=251=$素数 であることが確定した．——

この例の場合，$\sqrt{251}$ 以下の素数で割り算を実行する方が楽に，251＝素数，である判定が出来る．しかし，N が 50 桁，100 桁と大きくなった場合，$\sqrt{N}$ 以下の数で割り算をすることは，高速な計算機でも不可能である．しかし，この方法を用いると，もし $N-1$ が素因子分解出来るならば，能率よく判定出来る．N が 10 進法で 100 桁であっても，2 進法では 3 倍の 300 桁程度であるから，300 の何倍かの掛け算，割り算で判定出来るからである．

§4 ルカステストの拡張

もし $N+1$ が素因子分解されたならば，N が素数か否か判定出来る．ルカステストにおいては $N=M_p=2^p-1$ のときの素数か否かの判定法であった．$N=M_p$ のとき $N+1=M_p+1=2^p$ となり，2 の巾となり，素因子分解されている．このルカステストに用いられている技法を利用すると，次のような判定法が得られる．

$N+1$ は素因子分解されているとする．整数 a, b を

(1) $$(N, 2ab(a^2+4b)) = 1$$

(2) $$\left(\frac{a^2+4b}{N}\right) = -1$$

となるように選ぶ．(2)はヤコビの記号である．数列 y_n を

(3) $$y_0 = 0, \qquad y_1 = 1, \qquad y_{n+1} = ay_n + by_{n-1}$$

で定義する．$a=1, b=1$ のときがフィボナッチ数列である．このとき

(4) $$N = \text{素数} \Longrightarrow y_{N+1} \equiv 0 \pmod{N}$$

が成り立つ．よって $y_{N+1}\not\equiv 0 \pmod N$ ならば，N は合成数である．$y_{N+1}\equiv 0 \pmod N$ でもすぐには，N＝素数，と判定出来ないが．

(5) $$y_{N+1}\equiv 0 \pmod N$$

(6) $N+1$ のどの素因子 p に対しても $(y_{(N+1)/p}, N)=1$

であるならば，N＝素数，と判定される．

以上のことを順に証明しよう．まず，方程式

(7) $$x^2-ax-b=0$$

の根を α, β とすると，$D=a^2+4b$，とおいたとき

$$\alpha=\frac{a+\sqrt{D}}{2},\qquad \beta=\frac{a-\sqrt{D}}{2},\qquad D=a^2+4b$$

となる．α, β から y_n を表わすと

(8) $$y_n=(\alpha^n-\beta^n)/\sqrt{D}$$

となる．証明は帰納法で出来る．$n=0$ のときは $y_0=0, (\alpha^0-\beta^0)/\sqrt{D}=(1-1)/\sqrt{D}=0$ から成り立つ．$n=1$ のときは $y_1=1, (\alpha^1-\beta^1)/\sqrt{D}=(\alpha-\beta)/\sqrt{D}=1$ から成り立つ．y_n, y_{n-1} に対して成り立つとすると

$$\begin{aligned} y_{n+1} &= ay_n+by_{n-1} \\ &= \{a(\alpha^n-\beta^n)+b(\alpha^{n-1}-\beta^{n-1})\}/\sqrt{D} \\ &= \{\alpha^{n-1}(a\alpha+b)-\beta^{n-1}(a\beta+b)\}/\sqrt{D}. \end{aligned}$$

α も β も (7) の根であるから $a\alpha+b=\alpha^2$，$a\beta+b=\beta^2$ となり

$$\begin{aligned} y_{n+1} &= \{\alpha^{n-1}\cdot\alpha^2-\beta^{n-1}\cdot\beta^2\}/\sqrt{D} \\ &= (\alpha^{n+1}-\beta^{n+1})/\sqrt{D} \end{aligned}$$

から (8) が成り立つことがわかった．

次に，数列 x_n を

(9) $$x_0=2,\qquad x_1=a,\qquad x_{n+1}=ax_n+bx_{n-1}$$

で定義すると (8) と同様に

(10) $$x_n=\alpha^n+\beta^n$$

が得られる. $n=0$ のとき $\alpha^0+\beta^0=1+1=2=x_0$ となる. $n=1$ のとき $\alpha^1+\beta^1=\alpha+\beta=a=x_1$ となる. x_n, x_{n-1} に対して成り立つとき

$$\begin{aligned} x_{n+1} &= ax_n+bx_{n-1} \\ &= a(\alpha^n+\beta^n)+b(\alpha^{n-1}+\beta^{n-1}) \\ &= \alpha^{n-1}(a\alpha+b)+\beta^{n-1}(a\beta+b) \\ &= \alpha^{n-1}\cdot\alpha^2+\beta^{n-1}\cdot\beta^2 \\ &= \alpha^{n+1}+\beta^{n+1} \end{aligned}$$

となり, (10) が成り立つことが示された.

(8) と (10) から多くの式を示すことが出来る. たとえば

(11) $$x_n = y_{n+1}+by_{n-1}.$$

右辺を (8) を使い変形すると

$$右辺 = \{\alpha^{n+1}-\beta^{n+1}+b(\alpha^{n-1}-\beta^{n-1})\}/\sqrt{D}.$$

$b=-\alpha\beta$ であるから

$$\begin{aligned} &= \{\alpha^{n+1}-\beta^{n+1}-\alpha\beta(\alpha^{n-1}-\beta^{n-1})\}/\sqrt{D} \\ &= \{\alpha^{n+1}-\beta^{n+1}-\alpha^n\beta+\alpha\beta^n\}/\sqrt{D} \\ &= \{\alpha^n(\alpha-\beta)+\beta^n(\alpha-\beta)\}/\sqrt{D}. \end{aligned}$$

$\alpha-\beta=\sqrt{D}$ であるから

$$\begin{aligned} &= \alpha^n+\beta^n \\ &= 左辺. \end{aligned}$$

(12) $$y_{m+n} = y_m y_{n+1}+by_{m-1}y_n.$$

$$\begin{aligned} 右辺 &= \{(\alpha^m-\beta^m)(\alpha^{n+1}-\beta^{n+1})-\alpha\beta(\alpha^{m-1}-\beta^{m-1})(\alpha^n-\beta^n)\}/D \\ &= (\alpha^{m+n+1}-\alpha^m\beta^{n+1}-\alpha^{n+1}\beta^m+\beta^{m+n+1} \\ &\quad -\alpha^{m+n}\beta+\alpha^m\beta^{n+1}+\alpha^{n+1}\beta^m-\alpha\beta^{m+n})/D \\ &= \{\alpha^{m+n}(\alpha-\beta)-\beta^{m+n}(\alpha-\beta)\}/D \\ &= (\alpha^{m+n}-\beta^{m+n})/\sqrt{D} \\ &= 左辺. \end{aligned}$$

また (8), (10) を 2 項定理で展開すると

$$(13)\quad y_n=\left\{\left(\frac{a+\sqrt{D}}{2}\right)^n-\left(\frac{a-\sqrt{D}}{2}\right)^n\right\}\Big/\sqrt{D}$$

$$=\frac{1}{2^n\sqrt{D}}\left\{\sum_i\binom{n}{i}a^{n-i}\sqrt{D}^{\,i}-\sum_i\binom{n}{i}a^{n-i}(-\sqrt{D})^i\right\}$$

$$=\frac{1}{2^n\sqrt{D}}\left\{2\sum_k\binom{n}{2k+1}a^{n-2k-1}\cdot D^k\sqrt{D}\right\}$$

$$=\frac{1}{2^{n-1}}\cdot\sum_k\binom{n}{2k+1}a^{n-2k-1}D^k.$$

$$(14)\quad x_n=\left(\frac{a+\sqrt{D}}{2}\right)^n+\left(\frac{a-\sqrt{D}}{2}\right)^n$$

$$=\frac{1}{2^n}\left\{\sum_i\binom{n}{i}a^{n-i}\sqrt{D}^{\,i}+\sum_i\binom{n}{i}a^{n-i}(-\sqrt{D})^i\right\}$$

$$=\frac{1}{2^n}\left\{2\sum_k\binom{n}{2k}a^{n-2k}D^k\right\}$$

$$=\frac{1}{2^{n-1}}\cdot\sum_k\binom{n}{2k}a^{n-2k}D^k.$$

以上で準備が終った．まず(4)を証明しよう．

N が素数ならば，オイラーの規準から

$$\left(\frac{D}{N}\right)\equiv D^{(N-1)/2}\pmod{N}$$

となり，(2)からこの値は -1 と合同となる．また

$$\binom{N+1}{2k+1}=\binom{N}{2k+1}+\binom{N}{2k}$$

であるが，$2k+1\neq N$, $2k+1\neq 1$ ならば右辺の 2 つの項は N で割り切れる．フェルマーの定理から

$$2^{N-1}\equiv 1\pmod{N}$$

$$a^{N-1}\equiv 1\pmod{N}$$

であるから(13)から mod N で計算すると

$$y_{N+1}\equiv\frac{2^{N-1}\cdot 2^{N-1}}{2^N}\sum_k\binom{N+1}{2k+1}a^{N+1-2k-1}D^k$$

$$
\begin{aligned}
&\equiv 2^{N-2}\left\{\binom{N+1}{1}a^N+\binom{N+1}{N}\cdot a\cdot D^{(N-1)/2}\right\}\\
&=2^{N-2}a\{(N+1)a^{N-1}+(N+1)\cdot D^{(N-1)/2}\}\\
&\equiv 2^{N-2}a(a^{N-1}+D^{(N-1)/2})\\
&\equiv 0
\end{aligned}
$$

となり，(4)が示された．

逆に(5), (6)が成り立っているとする．qをNの素因子とすれば$(q, 2abD)=1$である．また$\binom{q}{2k+1}$は$2k+1\neq q$ならばqで割れる．$\binom{q}{2k}$も$k\neq 0$ならばqで割れる．よって(13), (14)から mod q で計算すると

$$
\begin{aligned}
y_q &\equiv \frac{2^{q-1}}{2^{q-1}}\sum_k\binom{q}{2k+1}a^{q-2k-1}D^k\\
&\equiv D^{(q-1)/2}\\
x_q &\equiv \frac{2^{q-1}}{2^{q-1}}\sum_k\binom{q}{2k}a^{q-2k}D^k\\
&\equiv a^q\\
&\equiv a
\end{aligned}
$$

となる．$D^{q-1}\equiv 1 \pmod q$から$D^{(q-1)/2}\equiv\pm 1 \pmod q$であるが，もし$D^{(q-1)/2}\equiv -1 \pmod q$ならば$y_q\equiv -1 \pmod q$となり(3), (11)から

$$
\begin{aligned}
y_{q+1} &= ay_q+by_{q-1}\\
&= ay_q+x_q-y_{q+1}\\
&\equiv -a+a-y_{q+1} \pmod q\\
&= -y_{q+1}
\end{aligned}
$$

となり，$q\neq 2$から$y_{q+1}\equiv 0 \pmod q$が得られる．もし$D^{(q-1)/2}\equiv 1 \pmod q$ならば，$y_q\equiv 1 \pmod q$となり(3), (11)から

$$
by_{q-1} = -ay_q+y_{q+1}
$$

$$= -ay_q + x_q - by_{q-1}$$
$$\equiv -a + a - by_{q-1} \pmod q$$
$$= -by_{q-1}$$

となる．q は b の約数ではないから，$y_{q-1} \equiv 0 \pmod q$ が得られた．まとめると

(15)　$y_{q+1} \equiv 0$　または　$y_{q-1} \equiv 0 \pmod q$

となる．ところで，$y_n \equiv 0 \pmod q$ となる n のうち，最小の自然数を m とすると，(15) から $m \leqq q+1$ となる．また

(16)　$y_n \equiv 0 \pmod q \Longleftrightarrow m|n$

が言える．なぜならば(12)から

(17)
$$\begin{aligned} y_{m+k} &= y_{(m+1)+(k-1)} \\ &= y_{m+1}y_k + by_my_{k-1} \\ &\equiv y_{m+1}y_k \pmod q \end{aligned}$$

となる．もし $q|y_{m+1}$ ならば $q|y_m$, $(q,b)=1$ と漸化式(3)から $q|y_{m-1}$ が得られ，この操作を続けると $q|y_1=1$ となり，矛盾である．よって $(q, y_{m+1})=1$ となる．もし $q|y_{m+k}$ ならば(17)から $q|y_k$ となる．つまり $q|y_n$ ならば $q|y_{n-m}$ となる．$q|y_n$ となる n のうち最小な自然数が m であったから $q|y_n$ ならば $m|n$ が得られる．逆に(17)において $k=m$ とすると $q|y_{2m}$ となる．次に $k=2m$ とおけば $q|y_{3m}$ となる．同様にして $m|n$ ならば $q|y_n$ が得られる．

さて，(5), (6) から

(18)　$y_{N+1} \equiv 0 \pmod q$

(19)　$N+1$ のどの素因子 p に対しても $y_{(N+1)/p} \not\equiv 0 \pmod q$

が得られるから，$m=N+1$ にならざるを得ない．このとき，q は N の素因子であるから

$$N+1 = m \leqq q+1 \leqq N+1$$

となり $N=q$，つまり，$N=$素数，となることが確定する．

以上でルカステストの拡張の証明は終った．次に実際には，どのように能率的に y_n を計算するか示そう．

まず，2倍角の公式については(12)と(3)から

$$(20) \qquad \begin{aligned} y_{2n} &= y_n y_{n+1} + b y_{n-1} y_n \\ &= y_n y_{n+1} + (y_{n+1} - a y_n) y_n \\ &= 2 y_n y_{n+1} - a {y_n}^2 \end{aligned}$$

が得られる．また，同様に

$$(21) \qquad \begin{aligned} y_{2n+1} &= y_{(n+1)+n} \\ &= y_{n+1} y_{n+1} + b y_n y_n \\ &= {y_{n+1}}^2 + b {y_n}^2 \end{aligned}$$

が得られる．(3)を使えば

$$(22) \qquad \begin{aligned} y_{2n+2} &= a y_{2n+1} + b y_{2n} \\ &= a({y_{n+1}}^2 + b {y_n}^2) + b(2 y_n y_{n+1} - a {y_n}^2) \\ &= a {y_{n+1}}^2 + 2b y_n y_{n+1} \end{aligned}$$

となる．つまり対(y_n, y_{n+1})から対(y_{2n}, y_{2n+1})または対(y_{2n+1}, y_{2n+2})が得られる．この計算をつみ重ねれば，能率よく y_n が計算出来る．

例　$N=247$ のとき $N+1$ を2進法で表わすと $N+1=11111000$ となる．よって次のように y_{N+1} を mod N で計算する．

まず $a=1$, $b=1$ とすると

$$\left(\frac{5}{247}\right) = \left(\frac{247}{5}\right) = \left(\frac{2}{5}\right) = -1$$

から(1), (2)は満足される．mod 247 で計算すると

$$y_0 = 0,\ y_1 = 1,\ y_2 = 1,\ y_3 = 2,\ y_4 = 3,\ y_5 = 5,$$
$$y_6 = 8,\ y_7 = 13,\ y_8 = 21$$
$$y_{15} = {y_8}^2 + {y_7}^2 \equiv 116$$
$$y_{16} = {y_8}^2 + 2 y_7 y_8 \equiv 246$$
$$y_{31} = {y_{16}}^2 + {y_{15}}^2 \equiv 119$$

$$y_{32} = {y_{16}}^2 + 2y_{15}y_{16} \equiv 16$$
$$y_{62} = 2y_{31}y_{32} - {y_{31}}^2 \equiv 21$$
$$y_{63} = {y_{32}}^2 + {y_{31}}^2 \equiv 91$$
$$y_{124} = 2y_{62}y_{63} - {y_{62}}^2 \equiv 170$$
$$y_{125} = {y_{63}}^2 + {y_{62}}^2 \equiv 77$$
$$y_{248} = 2y_{124}y_{125} - {y_{124}}^2 \equiv 244 \not\equiv 0 \pmod{247}.$$

よって，247 は素数ではない．——

§5　素因子分解法

方法 1　或る自然数 N が与えられたとき，N を素因子分解するにはどうしたらよいだろうか．一番素朴な方法は小さな素数の順に割っていけばよい．もし $\sqrt{N}$ 以下の最大の素数まで割っていっても，割り切れなければ N は素数である．

方法 2　次に手近に素数表がないとき，または簡単なプログラムを組み電卓などで素因子を求めるときなどは，小さい数の順に割っていけばよい．N が奇数のときは，小さな奇数の順に割っていけば計算量は半分になる．N が 2, 3, 5, 7 で割れないときは，3, 5, 7 の倍数でない奇数で割っていけば，計算量はさらに半分以下になる．なぜならば，$2\times3\times5\times7=210$ であり，1 から 210 までの中に 2, 3, 5, 7 で割れない数の個数は

$$\varphi(210) = (2-1)(3-1)(5-1)(7-1) = 48 < \frac{210}{4}$$

となるからである．2, 3, 5, 7 の倍数をどのように除くかといえば，まず，1 から 211 までの奇数を並べ，3, 5, 7 の倍数を除いてみる．

1	~~3~~	~~5~~	~~7~~	~~9~~	11	13	~~15~~	17	19
~~21~~	23	~~25~~	~~27~~	29	31	~~33~~	~~35~~	37	~~39~~
41	43	~~45~~	47	~~49~~	~~51~~	53	~~55~~	~~57~~	59

61	~~63~~	~~65~~	67	~~69~~	71	73	~~75~~	~~77~~	79
~~81~~	83	~~85~~	~~87~~	89	~~91~~	~~93~~	~~95~~	97	~~99~~
101	103	~~105~~	107	109	~~111~~	113	~~115~~	~~117~~	~~119~~
121	~~123~~	~~125~~	127	~~129~~	131	~~133~~	~~135~~	137	139
~~141~~	143	~~145~~	~~147~~	149	151	~~153~~	~~155~~	157	~~159~~
~~161~~	163	~~165~~	167	169	~~171~~	173	~~175~~	~~177~~	179
181	~~183~~	~~185~~	187	~~189~~	191	193	~~195~~	197	199
~~201~~	~~203~~	~~205~~	~~207~~	209	211				

残った 49 個の数の間隔は，1 から出発すると

10	2	4	2	4	6	2	6	4	2	4	6
6	2	6	4	2	6	4	6	8	4	2	4
2	4	8	6	4	6	2	4	6	2	6	6
4	2	4	6	2	6	4	2	4	2	10	2

となる．よってまず 1 に 10 を加えた 11 で割る．次に 2 を加えた 13 で割る．次に 4 を加えた 17 で割る．以下同様にしていけば，48 個を周期として，3, 5, 7 で割れない奇数が小さい順にすべて現われる．

以上の原始的な方法で，素因子がなかなか見つからないときは，いろいろな工夫が考え出されている．ここではフェルマーの方法とルジャンドルの方法を紹介しよう．

方法 3　まず N が奇数とし，

$$N = a \cdot b, \qquad a \leqq b$$

と分解したとする．N が奇数だから a, b も奇数となり

$$x = \frac{b+a}{2}, \qquad y = \frac{b-a}{2}$$

とおけば，x, y は整数となる．このとき

$$x^2-y^2=\frac{(b+a)^2}{4}-\frac{(b-a)^2}{4}=ab=N$$

となる．よってこのような x, y を見つければよい（フェルマーの方法）．そのためには，はじめに，$x=[\sqrt{N}]$，$y=0$ から出発し

(1)
$$r=x^2-y^2-N$$

が0になるように x, y を調節すればよい．もし r が負ならば，x の値を1つ殖やし，r が正ならば，負になるまで y の値を1つずつ殖やせばよい．$r=0$ となる x, y が見つかれば $N=(x+y)(x-y)$ と分解されるわけである．$x_1=2x+1$，$y_1=2y+1$ とおけば，x の値を1つ殖やすときは，r の値が x_1 だけ殖え，x_1 の値は2だけ殖える．y の値を1つ殖やすことは，r の値が y_1 だけ減り，y_1 の値は2だけ殖える，つまり，足し算と引き算をくり返していけばよい．

例　$N=8633$ のとき $[\sqrt{N}]=92$ であるから

$$r=92^2-8633=-169$$
$$x_1=2\cdot x+1=185$$
$$y_1=2\cdot y+1=1$$

から出発する．r が負であるから x_1 を加え，そのあとで x_1 の値を2殖やす．よって，r, x_1 は

$$r=-169+185=16$$
$$x_1=185+2=187$$

となる．r が正になったので，y_1 を引き，その後 y_1 の値を2殖やす．以下同様に続けると，r, x_1, y_1 の値は表9-1のように変化する．

よって $x=(187-1)/2=93$，$y=(9-1)/2=4$ となり

$$N=93^2-4^2$$
$$=(93+4)(93-4)$$
$$=97\cdot 89$$

と2つの因子に分解した．

表 9-1

r	x_1	y_1
-169	185	1
16	187	1
15	187	3
12	187	5
7	187	7
0	187	9

この方法は N の因子が $\sqrt{N}$ に近いと因子が早く見つかる．

方法 4　さて $N=x^2-y^2$ とならなくとも

$$x^2 \equiv y^2 \pmod N \tag{2}$$

となる x と y が見つかると，N の分解が得られる可能性がある．なぜならば，$x^2-y^2=(x+y)(x-y)$ が N で割れるので，もし，$x+y, x-y$ が共に N で割れなければ，$x-y$ と N の最大公約数を求めれば，N の真の約数が見つかる．(2) のような x, y を見つけるために，ペル方程式

$$x^2-Ny^2 = \pm 1$$

の解を求める計算法を利用する．定理 21 において $\alpha_i=p_i+q_i\sqrt{N}$ とおくと

$$p_i{}^2-Nq_i{}^2 = (-1)^i\cdot b_i$$

であるから

$$p_i{}^2 \equiv (-1)^i b_i \pmod N$$

となる．よって $(-1)^i b_i$ またはいくつかの $(-1)^i b_i$ の積が平方数になれば，(2) のような x, y が見つかる（ルジャンドルの方法）．

例　$N=20099$ とすると，第 8 章 §8 の計算から

$$p_1 = 141 \qquad b_1 = 218$$
$$p_2 = 142 \qquad b_2 = 65$$

$$p_3 = 567 \qquad b_3 = 95$$
$$p_4 = 1276 \qquad b_4 = 157$$
$$p_5 = 1843 \qquad b_5 = 82$$
$$p_6 = 4962 \qquad b_6 = 169 = 13^2$$

となる．よって

$$4962^2 \equiv 13^2 \pmod{20099}$$

が得られ，

$$4962^2 - 13^2 = (4962+13)(4962-13)$$
$$= 4975 \cdot 4949$$

となる．

$$20099 = 4949 \times 4 + 303$$
$$4949 = 303 \times 16 + 101$$
$$303 = 101 \times 3$$
$$\therefore \quad (20099, 4949) = 101$$

であるから，N の約数 101 が見つかり，

$$N = 101 \times 199$$

と分解出来た．——

この方法を用いて F_7 の分解

$$F_7 = 2^{2^7} + 1$$
$$= 59649589127497217 \times 5704689200685129054721$$

が得られた(1970)．

その他，いろいろな工夫が考え出されている．しかし，一般に運がよくなければ，大きな N の分解はうまくいかない．たとえば，N が 50 桁の素数×50 桁の素数，となると，高速計算機を用いても絶望的である．

§6 素数と暗号

整数論が実社会において利用されるようになってきた．今，話題になっているのは秘密にすべき文章を安全に相手に伝えるには，大きな素数を利用するとよい，ということである．つまり，伝えるべき文章を暗号化するとき，素数を利用すると，その暗号文を受け取った人以外には決して暗号文が復元出来ない，という方法である．

文章を送信するには，まずその文章を数字の列に直す．これを**符号化**という．この符号化は暗号化とはちがう．たとえば“あ，い，う，え，お，…”に対して“01, 02, 03, 04, 05, …”という数字を対応させれば，文字は句読点を含めても100字以下であるから，1文字には2つの数が対応し，50字以内の文章にはそれらの数を1列に並べた100桁以内の数が対応する．

例 “家”には“いえ”を符号化して“0204”という数を対応させる．——

このように符号化された数xがわかれば，容易に元の文章は得られる．よって，たとえば100桁以内の数xをいかに安全に送信するか，が問題となる．

今，pとqを50桁ほどの相異なる素数としよう．$N=p\cdot q$とすれば，$\varphi(N)=(p-1)(q-1)$となる．rを$(r,\varphi(N))=1$となる自然数とすれば

$$(1) \qquad r\cdot s\equiv 1 \pmod{\varphi(N)}$$

となるsは$\bmod \varphi(N)$でただ1つ定まる．

さて，Nとrは送信者に教える．しかしsは受信者だけの秘密にする．送信者はxに対して

$$x^r\equiv y \pmod N \qquad (0<y<N)$$

となるyを計算する．これを**暗号化**という．受信者は，yという値を受け取り，xを計算する．(1)から

$$r\cdot s = k\cdot\varphi(N)+1$$

となる自然数 k が定まる．オイラーの定理から

$$\begin{aligned} y^s &\equiv (x^r)^s \pmod N \\ &= (x^{\varphi(N)})^k\cdot x \\ &\equiv x \pmod N \end{aligned}$$

となるので，$0<x<N$ ならば y から x を計算することが出来る．これを**復号化**という．受信者はこのように暗号を解読することが出来る．

では，y という値および N と r の値がスパイに伝わってしまったとしよう．スパイは N, r, y の3つの値から x の値を求めようと努力するであろう．しかし，N は100桁もある大きな数である．素因子に分解することは，事実上不可能である．よって $\varphi(N)$ の値もわからず，s の値もわからない．つまり解読出来ない．

この暗号の面白さは，N と r が公開されていても，つまり，暗号化の方法がわかっていても，復号化することが出来ない，つまり送信者にも復号化がわからない，という点である．よって，二重に安全な方法である．

素数か否かの判定は出来ても，素因子分解が非常に困難であることを利用した面白い方法である．

第10章　素数を表わす多項式

素数を小さい順に並べ

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ p_5 = 11,\ \cdots$$

としたとき，n 番目の素数 p_n を n の関数として具体的に表わせないだろうか．また p_n までわかったとき，素数 p_{n+1} を p_n を使って具体的に表わせないだろうか．もし表わせたならば，素数に関する多くの問題が解決するであろう．しかし素数はあまりにも不規則に並んでいるので，これらの式は作れそうもない．では素数しか表わさない式は作れないだろうか．前にも述べた通りフェルマーは

$$F_n = 2^{2^n}+1, \qquad n = 0, 1, 2, \cdots$$

はすべて素数であろうと予想したが，F_5 が素数でないことをオイラーが見つけ，予想が外れた．今までのところ素数しか表わさない式は作られていない．オイラーは

$$f(n) = n^2+n+41$$

という2次式が $n=0, 1, 2, \cdots, 39$ に対して素数値になることをみつけた．しかし $n=40$ では $f(40)=41^2$ となり，この式が素数ばかり表わすわけではないことがわかった．このように素数を表わす式の歴史は失敗とあきらめの歴史であった．ところが1971年，ソ連のマチアセビッチは素数または負の整数しか表わさない多項式を作り出した．この多項式はすべての素数を表わすことが出来る．この章ではこの多項式を具体的に作り，すべての素数を表わすことを証明しよう．

§1　定義と目的

素数を表わす多項式 $f(x_1, x_2, \cdots, x_n)$ とは，整数係数の多項式で，次の2つの性質を持つものである．

(1) $x_1, x_2, \cdots, x_n$ に自然数の値を代入したとき，$f(x_1, x_2, \cdots x_n)$ が正ならば $f(x_1, x_2, \cdots, x_n)$ は素数である．

(2) どのような素数 p に対しても，適当に自然数 $x_1, x_2, \cdots, x_n$ を選ぶと $p=f(x_1, x_2, \cdots, x_n)$ となる．

本章の目的は具体的に $f(x_1, x_2, \cdots, x_n)$ を作ることである．そのためには次の2つの性質を持つ整数係数の多項式 $g(x_1, x_2, \cdots, x_n)$ を作ればよい(H. Putnum[6])．

(3) $x_1, x_2, \cdots, x_n$ に自然数の値を代入したとき，$g(x_1, x_2, \cdots, x_n)=0$ であれば x_1+1 は素数である．

(4) どのような素数 x_1+1 に対しても適当に自然数 $x_2, x_3, \cdots, x_n$ を選ぶと $g(x_1, x_2, \cdots, x_n)=0$ となる．

何故ならば，もしこのような $g(x_1, x_2, \cdots, x_n)$ が作れたとするとき

$$f(x_1, x_2, \cdots, x_n) = (x_1+1)(1-g^2(x_1, x_2, \cdots, x_n))$$

とおく．$x_1, x_2, \cdots, x_n$ に自然数の値を代入したとき，$f(x_1, x_2, \cdots, x_n)$ が正ならば x_1+1 は正だから $1-g^2(x_1, x_2, \cdots, x_n)$ も正でなければならない．$g(x_1, x_2, \cdots, x_n)$ の係数は整数だから，$x_1, x_2, \cdots, x_n$ が自然数のとき $g(x_1, x_2, \cdots, x_n)$ は整数である．よって，その自乗である $g^2(x_1, x_2, \cdots, x_n)$ は0または自然数である．よって $1-g^2(x_1, x_2, \cdots, x_n)$ が正であるためには $g(x_1, x_2, \cdots, x_n)=0$ でなければならない．よって(3)から，$x_1+1=$素数，である．このとき

$$\begin{aligned} f(x_1, x_2, \cdots, x_n) &= (x_1+1)(1-g^2(x_1, x_2, \cdots, x_n)) \\ &= (x_1+1)(1-0^2) \\ &= x_1+1 = \text{素数} \end{aligned}$$

つまり(1)が示された．次にどのような素数 p に対しても，$x_1=p-1$

とおけば(4)から適当な自然数 $x_2, \cdots, x_n$ を選ぶと $g(x_1, x_2, \cdots, x_n)=0$ となる．このとき

$$f(x_1, x_2, \cdots, x_n) = (x_1+1)(1-g^2(x_1, x_2, \cdots, x_n))$$
$$= (x_1+1)(1-0^2) = x_1+1 = p$$

つまり(2)が示された．

$f(x_1, x_2, \cdots, x_n)$ から素数 p を得るために $x_1=p-1$ とおくのだから，どこかでごまかされたような気持になる．あらかじめその素数の値を知っていなければならないからである．しかし(3), (4)の性質を持つ多項式が存在することは驚異的なことである．

§2　ウィルソンの定理と素数を表わす多項式

ウィルソンの定理によると，p が 2 以上の自然数のとき

$$p = \text{素数} \Longleftrightarrow (p-1)! \equiv -1 \pmod p$$

となる．よって，自然数 x_1 に対して次の 2 つの性質が成立する．

(1)　$x_1!+1$ が x_1+1 で割り切れれば x_1+1 は素数である．

(2)　x_1+1 が素数ならば $x_1!+1$ は x_1+1 で割り切れる．

さて，次の性質を持つ整係数の多項式 $h(x_1, x_2, \cdots, x_{n-1})$ が作れたとする．

(3)　$x_1, x_2, \cdots, x_{n-1}$ に自然数の値を代入したとき $h(x_1, x_2, \cdots, x_{n-1})=0$ であれば $x_2=x_1!$ である．

(4)　自然数 x_1, x_2 に対して，もし $x_2=x_1!$ であるならば，適当に自然数 $x_3, \cdots, x_{n-1}$ を選ぶと $h(x_1, x_2, x_3, \cdots, x_{n-1})=0$ となる．

このとき

$$g(x_1, x_2, \cdots, x_n) = \{(x_1+1)x_n-(x_2+1)\}^2+h^2(x_1, x_2, \cdots, x_{n-1})$$

とおく．もし $g(x_1, x_2, \cdots, x_n)=0$ ならば

(5)　$$(x_1+1)x_n-(x_2+1) = 0$$

(6)　$$h(x_1, x_2, x_3, \cdots, x_{n-1}) = 0$$

でなければならない．(3)と(6)から，$x_2=x_1!$ となる．(5)から $x_1!+1$ が x_1+1 で割り切れる．よって(1)から，$x_1+1=$素数 となる．つまり§1(3)が成立した．次に，$x_1+1=$素数 とすると，(2)から $x_1!+1$ は x_1+1 で割り切れる．よって $x_2=x_1!$ とおくと $(x_2+1)=(x_1+1)x_n$ となる自然数 x_n が定まる．また(4)から適当に $x_3, \cdots, x_{n-1}$ を定めると $h(x_1, x_2, x_3, \cdots, x_{n-1})=0$ となる．これら $x_2, x_3, \cdots, x_n$ を $g(x_1, x_2, \cdots, x_n)$ に代入すると(5), (6)が成立するので $g(x_1, x_2, \cdots, x_n)=0$ となる．つまり§1(4)が成立した．

まとめると(3), (4)を満たす多項式 $h(x_1, x_2, \cdots, x_{n-1})$ から素数を表わす多項式 $f(x_1, x_2, \cdots, x_n)$ が作られる．

ウィルソンの定理を使わなくとも素数の定義にもどれば，2以上の自然数 p が素数であることは，1と p 以外に p の約数がないことだから

$$p=\text{素数} \Longleftrightarrow (p, (p-1)!)=1.$$

このとき，定理2から適当な整数 y, z で

$$py+(p-1)!z=1$$

となる．よって y か z のどちらかは正だが，もう片方が負にならないと，左辺は1とならない．よって

$$\begin{aligned} p=\text{素数} &\Longleftrightarrow \text{適当な自然数 } x_n, x_{n+1} \text{ に対して} \\ &\qquad px_n-(p-1)!x_{n+1}=1 \text{ または } -1 \text{ となる.} \\ &\Longleftrightarrow \text{適当な自然数 } x_n, x_{n+1} \text{ に対して} \\ &\qquad (px_n-(p-1)!x_{n+1})^2=1. \end{aligned}$$

よって変数が1つ多くなるが

$$\begin{aligned} &g(x_1, x_2, \cdots, x_{n+1}) \\ &\quad =\{((x_1+1)x_n-x_2x_{n+1})^2-1\}^2+h^2(x_1, x_2, \cdots, x_{n-1}) \end{aligned}$$

としても素数を表わす多項式は作れる．つまり，素数を表わす多項式 $f(x_1, x_2, \cdots, x_n)$ を作るためには，素数に関する性質は素数の定義

以外何も使われていない．よって $f(x_1, x_2, \cdots, x_n)$ から素数に関する知識は何も期待出来ない．たとえば $f(x_1, x_2, \cdots, x_n)$ に自然数の値を代入し，新しい大きな素数 p を作ろうとしても $x_2=(p-1)!$ でなければならず，x_2 を非常に大きくしなければならない．

次に(3), (4)を満たす多項式を作ろうと思う．証明はすべて初等的だけれど，少し長くなるので辛抱して読んでもらいたい．いくつかの部分に分けて順に証明していこうと思う．

§3　ペル方程式の解を表わす多項式

自然数 a が 1 より大きいとすると

$$(a-1)^2 = a^2-2a+1 < a^2-2+1 = a^2-1$$

$$\therefore\quad (a-1)^2 < a^2-1 < a^2.$$

よって a^2-1 は平方数ではない．よってペル方程式

$$(1)\qquad x^2-(a^2-1)y^2 = 1$$

は自然数解を無限に多く持つ．最小の自然数解は $x=a, y=1$ である．よってすべての解を y の小さい順に並べ $y_1=1<y_2<y_3<\cdots$ とするとそれらは

$$(2)\qquad (a+\sqrt{a^2-1})^n = x_n+\sqrt{a^2-1}\,y_n$$

として計算出来る．たとえば $n=2$ のとき

$$(a+\sqrt{a^2-1})^2 = a^2+2a\sqrt{a^2-1}+a^2-1$$

から $x_2=2a^2-1, y_2=2a$ となる．$a=1$ のときは(1)の解は $x=1$ となり y は何でもよい．よって y の小さい順に並べると

$$(3)\qquad x_n = 1,\qquad y_n = n\qquad (a=1 \text{ の場合})$$

となる．どちらにしても

$$(4)\qquad x_1 = a,\qquad y_1 = 1,\qquad x_2 = 2a^2-1,\qquad y_2 = 2a$$

$$(5)\qquad y_1 < y_2 < y_3 < \cdots$$

$$(6)\qquad n \leqq y_n$$

が成立する．x_n, y_n の性質を調べるために，いくつかの補題を証明する．まず x_n, y_n から x_{n+1}, y_{n+1} が計算出来ることを示そう．

補題1
$$x_{n+1} = ax_n+(a^2-1)y_n$$
$$y_{n+1} = x_n+ay_n.$$

証明 $a>1$ のとき，(2) から
$$\begin{aligned} x_{n+1}+\sqrt{a^2-1}\,y_{n+1} &= (a+\sqrt{a^2-1})^{n+1} \\ &= (a+\sqrt{a^2-1})(a+\sqrt{a^2-1})^n \\ &= (a+\sqrt{a^2-1})(x_n+\sqrt{a^2-1}\,y_n) \\ &= ax_n+(a^2-1)y_n+\sqrt{a^2-1}(x_n+ay_n). \end{aligned}$$
よって求める式を得る．$a=1$ のときは (3) から
$$x_{n+1} = 1 = x_n = ax_n+(a^2-1)y_n$$
$$y_{n+1} = 1+n = 1+y_n = x_n+ay_n$$
となるのでやはり成り立つ．——

補題2 $x_{n+2} = 2ax_{n+1}-x_n$
$$y_{n+2} = 2ay_{n+1}-y_n.$$

証明 補題1の n を $n+1$ に変えれば
$$\begin{aligned} x_{n+2} &= ax_{n+1}+(a^2-1)y_{n+1} \\ &= ax_{n+1}+(a^2-1)(x_n+ay_n) \\ &= ax_{n+1}+a^2x_n-x_n+(a^2-1)ay_n \\ &= ax_{n+1}+a(ax_n+(a^2-1)y_n)-x_n \\ &= ax_{n+1}+ax_{n+1}-x_n \\ &= 2ax_{n+1}-x_n \end{aligned}$$
$$\begin{aligned} y_{n+2} &= x_{n+1}+ay_{n+1} \\ &= (ax_n+(a^2-1)y_n)+ay_{n+1} \\ &= ax_n+a^2y_n-y_n+ay_{n+1} \\ &= a(x_n+ay_n)-y_n+ay_{n+1} \\ &= ay_{n+1}-y_n+ay_{n+1} \end{aligned}$$

$$= 2ay_{n+1} - y_n. \text{ ——}$$

この補題と(4)から

$$y_3 = 2ay_2 - y_1 = 2a\cdot 2a - 1 = 4a^2 - 1$$
$$y_4 = 2ay_3 - y_2 = 2a(4a^2-1) - 2a = 8a^3 - 4a$$
$$\cdots$$

となり，一般に y_n は a の $n-1$ 次の整係数の多項式 $y_n(a)$ となる．同様に x_n は a の n 次の整係数の多項式 $x_n(a)$ となる．

補題 3　$(2a-1)^{n-1} \leqq y_n(a) \leqq (2a)^{n-1}$.

証明　数学的帰納法を用いて証明する．$n=1$ のとき 左辺$=1$, $y_1(a)=1$, 右辺$=1$. $n=2$ のとき 左辺$=2a-1$, $y_2(a)=2a$, 右辺$=2a$. よって $n=1, 2$ のときは成立する．n まで成り立つとすると

$$y_{n+1}(a) = 2ay_n - y_{n-1} < 2ay_n \leqq 2a(2a)^{n-1} = (2a)^n.$$

$y_{n-1} < y_n$ であるから

$$y_{n+1}(a) = 2ay_n - y_{n-1} > 2ay_n - y_n$$
$$= (2a-1)y_n \geqq (2a-1)(2a-1)^{n-1} = (2a-1)^n.$$

補題 4　$1 < a,\ 1 < n \Longrightarrow n + y_{n-1}(a) < y_n(a)$.

証明　$n=2$ のとき 左辺$=2+1=3$, 右辺$=2a \geqq 4$. よって成立する．n まで成り立つとすると

$$y_{n+1} = 2ay_n - y_{n-1} > 2ay_n - y_n = (2a-1)y_n$$
$$> 2y_n > y_n + n + y_{n-1} \geqq y_n + n + 1.$$

補題 5　$a \equiv b \pmod{m} \Longrightarrow x_n(a) \equiv x_n(b) \pmod{m}$

$$y_n(a) \equiv y_n(b) \pmod{m}.$$

特に $y_n(a) \equiv y_n(1) = n \pmod{a-1}$.

証明　$x_n(a), y_n(a)$ は a の整係数の多項式だから $a \equiv b \pmod{m}$ ならば合同式の性質から $x_n(a) \equiv x_n(b)$, $y_n(a) \equiv y_n(b) \pmod{m}$ となる．特に $a \equiv 1 \pmod{a-1}$ であるから(3)から $y_n(a) \equiv y_n(1) = n \pmod{a-1}$ となる．

補題 6　$a<b \Longrightarrow x_n(a)<x_n(b),\ \ y_n(a) \leqq y_n(b).$

証明　補題3から $y_n(a) \leqq (2a)^{n-1} \leqq (2(b-1))^{n-1}=(2b-2)^{n-1} \leqq (2b-1)^{n-1} \leqq y_n(b)$. よって $y_n(a) \leqq y_n(b)$ となる．この不等式を用いれば

$$\begin{aligned} x_n(a)^2 &= 1+(a^2-1)y_n(a)^2 \\ &< 1+(b^2-1)y_n(b)^2 = x_n(b)^2. \end{aligned}$$

よって $x_n(a)<x_n(b)$ となる．

補題 7

$$\begin{aligned} x_{n+m} &= x_n x_m+(a^2-1)y_n y_m \\ x_{n-m} &= x_n x_m-(a^2-1)y_n y_m \\ y_{n+m} &= x_n y_m+x_m y_n \\ y_{n-m} &= -x_n y_m+x_m y_n. \end{aligned}$$

証明　$a=1$ のとき $x_{n+m}=1$, $x_n x_m+(a^2-1)y_n y_m=1\cdot 1+0\cdot n\cdot m=1$. よって $x_{n+m}=x_n x_m+(a^2-1)y_n y_m$ となる．同様に $a=1$ のとき，他の3式も成立する．$a>1$ のとき，(2)から

$$\begin{aligned} x_{n+m}+\sqrt{a^2-1}\,y_{n+m} &= (a+\sqrt{a^2-1})^{n+m} \\ &= (a+\sqrt{a^2-1})^n(a+\sqrt{a^2-1})^m \\ &= (x_n+\sqrt{a^2-1}\,y_n)(x_m+\sqrt{a^2-1}\,y_m) \\ &= (x_n x_m+(a^2-1)y_n y_m)+\sqrt{a^2-1}(x_n y_m+x_m y_n). \end{aligned}$$

$$\begin{aligned} x_{n-m}+\sqrt{a^2-1}\,y_{n-m} &= (a+\sqrt{a^2-1})^{n-m} \\ &= \frac{(a+\sqrt{a^2-1})^n}{(a+\sqrt{a^2-1})^m} = \frac{x_n+\sqrt{a^2-1}\,y_n}{x_m+\sqrt{a^2-1}\,y_m}. \end{aligned}$$

分母に $x_m-\sqrt{a^2-1}\,y_m$ を掛けると，x_m, y_m がペル方程式 $x^2-(a^2-1)y^2=1$ の解であるから，1になるので

$$\begin{aligned} &= (x_n+\sqrt{a^2-1}\,y_n)(x_m-\sqrt{a^2-1}\,y_m) \\ &= (x_n x_m-(a^2-1)y_n y_m)+\sqrt{a^2-1}(-x_n y_m+x_m y_n). \end{aligned}$$

よって証明された．

補題 8

$$x_{2n}=2x_n{}^2-1$$

$$y_{2n} = 2x_n y_n.$$

証明 補題7において $n=m$ とおくと

$$\begin{aligned} x_{2n} &= x_{n+n} = x_n x_n + (a^2-1) y_n y_n \\ &= x_n^2 + x_n^2 - \{x_n^2 - (a^2-1) y_n^2\} \\ &= 2x_n^2 - 1 \\ y_{2n} &= y_{n+n} = x_n y_n + x_n y_n = 2x_n y_n. \text{ ——} \end{aligned}$$

さて，記号 $a|b$ はランダウの記号，つまり a は b の約数であることを表わすものとする.

補題 9 $$y_m^2 | y_n \Longrightarrow y_m | n.$$

証明 補題7から $y_n = y_{n-m+m} = x_{n-m} y_m + x_m y_{n-m}$ となるので，もし $y_m | y_n$ ならば $y_m | x_m y_{n-m}$ となる．また $x_m^2 - (a^2-1) y_m^2 = 1$ から $(x_m, y_m) = 1$ であるから $y_m | y_{n-m}$ となる．この操作をつづければ $y_m | y_{n-km}$. もし $n = km + r$, $0 < r < m$ ならば $y_m | y_r$ となり $0 < y_r < y_m$ に矛盾する．よって $y_m | y_n$ ならば $n = km$ となる．さて

$$\begin{aligned} x_{km} + \sqrt{a^2-1}\, y_{km} &= (a + \sqrt{a^2-1})^{km} \\ &= ((a + \sqrt{a^2-1})^m)^k \\ &= (x_m + \sqrt{a^2-1}\, y_m)^k \\ &= x_m^k + k x_m^{k-1} \cdot \sqrt{a^2-1}\, y_m + \cdots \end{aligned}$$

であるから $\sqrt{a^2-1}$ の係数を比較して

$$y_{km} = k x_m^{k-1} y_m + \binom{k}{3} x_m^{k-3} y_m^3 (a^2-1) + \cdots$$

となり，最初の1項以外は y_m^3 で割り切れる．よって

$$\begin{aligned} y_m^2 | y_{km} &\Longrightarrow y_m^2 | k x_m^{k-1} y_m \\ &\Longrightarrow y_m | k x_m^{k-1}. \end{aligned}$$

$(x_m, y_m) = 1$ であるから

$$\begin{aligned} &\Longrightarrow y_m | k \\ &\Longrightarrow y_m | km = n. \end{aligned}$$

補題 10　　$1<a,\ 1<n,\ x_i \equiv x_j \pmod{x_n}$

$$\Longrightarrow i \equiv \pm j \pmod{4n}.$$

証明　$x_{2n\pm m} = x_{2n}x_m \pm (a^2-1)y_{2n}y_m$　　(補題 7)

$= (2x_n{}^2-1)x_m \pm (a^2-1)\cdot 2x_ny_n\cdot y_m$　　(補題 8)

(7)　　$\therefore\quad x_{2n\pm m} \equiv -x_m \pmod{x_n}.$

$$x_{4n\pm m} = x_{2n+(2n\pm m)}$$

(8)　　$\therefore\quad x_{4n\pm m} \equiv -x_{2n\pm m} \equiv x_m \pmod{x_n}.$

よって x_i, x_j は $(\mathrm{mod}\ x_n)$ で考えるとき, $0<i, j\leqq 4n$ の場合の変化を調べればよい. 補題 1, $y_{n-1}\geqq y_1>0$, $a\geqq 2$ から

$$x_n = x_{n-1+1} = ax_{n-1}+(a^2-1)y_{n-1}$$

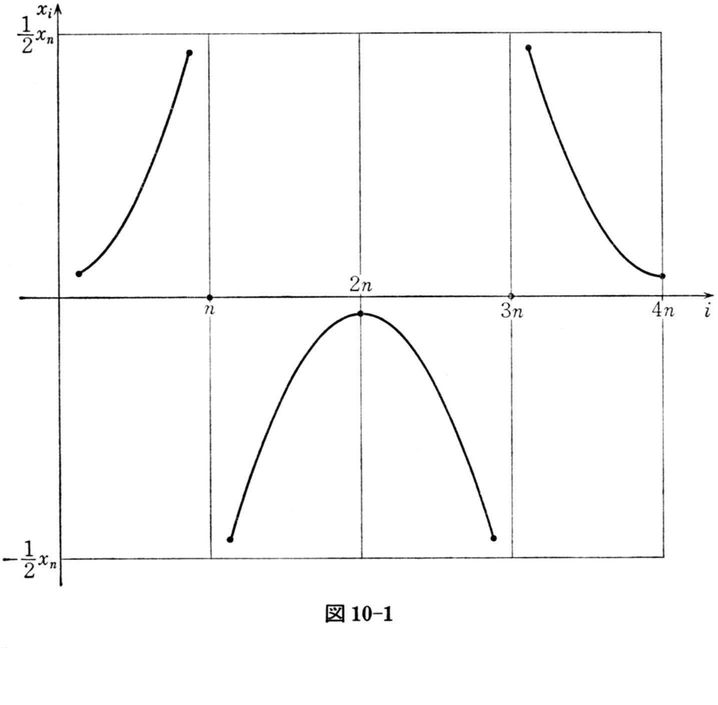


図 10–1

$$> ax_{n-1} \geqq 2x_{n-1}.$$

$$\therefore \quad x_{n-1} < \frac{1}{2}x_n.$$

$0<i\leqq 4n$ のときの $x_i \pmod{x_n}$ のグラフを(7), (8)を使って描くと，図10-1のようになる．このグラフにおいて，最大値と最小値の差は x_n より小さい．よって $0<i,\ j\leqq 4n$ のとき，$x_i\equiv x_j \pmod{x_n}$ ならばグラフ上の値は一致し，$i=j$ または $i+j=4n$ となる．よって一般の場合は $i\equiv \pm j \pmod{4n}$ となる．

補題 11　どのような自然数 $a,\ b$ に対しても $b|y_n(a)$ となる解 $y_n(a)$ が存在する．

証明　$a=1$ のときは $y_b(1)=b$ であるからよい．$a>1$ のときは

$$x^2-(a^2-1)b^2y^2=1$$

というペル方程式を考えると $(a^2-1)b^2$ は平方数ではないので $X>0,\ Y>0$ となる解がある．そのとき，X, bY は $x^2-(a^2-1)y^2=1$ の解である．つまり $bY=y_n(a)$ となる．——

さて，これだけの準備をして，この章の最大の見せ場である次の定理を証明しよう．

定理 27 (Matijasevič[4])　$1<a$ のとき自然数 y, n, a の関係が $y=y_n(a)$ となる必要十分条件は，次の条件を満たす自然数 b, c, d, e, g, x が存在することである．

i　$x^2-(a^2-1)y^2=1$

ii　$b^2-(a^2-1)C^2=1$

iii　$D^2-(F^2-1)E^2=1$

iv　$y=n+g-1$　（つまり $y\geqq n$）

ただし C, D, E, F は次のように定義される．

v　$C=2cy^2$

vi　$D=x+bd$

vii　$E = n+2(e-1)y$

viii　$F = a+b^2(b^2-a)$.

証明　もし i–viii を満たす自然数 b, c, d, e, g, x が存在したとする．このとき v から $C>1$，ii から $b^2>(a^2-1)+1=a^2>a$，viii から $F>a>1$，vi から $D>0$，vii から $E>0$．よって i, ii, iii から自然数 p, q, r が存在して

$$x = x_p(a), \qquad y = y_p(a)$$
$$b = x_q(a), \qquad C = y_q(a)$$
$$D = x_r(F), \qquad E = y_r(F)$$

となる．特に $C>1$ から $q>1$ となる．次に $p=n$ を示そう．

$(\mathrm{mod}\ 2y)$ で考えると v から $C\equiv 0$，ii から $b^2\equiv 1$，viii から $F\equiv 1$，補題 5 から $E=y_r(F)\equiv y_r(1)=r$，vii から $E\equiv n$，

$$\therefore \quad n \equiv r \pmod{2y}.$$

$(\mathrm{mod}\ b)$ で考えると viii から $F\equiv a$，補題 5 から $x_r(a)\equiv x_r(F)=D$，vi から $D\equiv x=x_p(a)$，$b=x_q(a)$ であるから $x_r(a)\equiv x_p(a) \pmod{x_q(a)}$ となる．$a>1, q>1$ と補題 10 から $r\equiv \pm p \pmod{4q}$ となる．他方 v から $y^2|C$，言い換えると $y_p(a)^2|y_q(a)$，補題 9 から $y_p(a)|q$，つまり $y|q$ となる．よって $2y|4q$ となるので $r\equiv\pm p \pmod{4q}$ から $r\equiv\pm p \pmod{2y}$ が得られる．

$$\therefore \quad n \equiv \pm p \pmod{2y}.$$

ところが iv から $n\leqq y$ であり，補題 6 から $p=y_p(1)\leqq y_p(a)=y$ であるからこの合同式から $n=p$ が得られる．つまり $y=y_n(a)$ となった．

逆に $y=y_n(a)$ のとき，$x=x_n(a)$ とおくと i が満たされる．(6) から iv を満たす g が存在する．補題 11 から $2y^2|y_q(a)$ となる自然数解 $y_q(a)$ があるので，$C=y_q(a)$ とおくと v を満たす c が存在する．$b=x_q(a)$ とおけば ii が満たされる．$F=a+b^2(b^2-a)$ とおけば viii は満たされる．このとき前半と同様にして $F>a>1$，$F\equiv 1 \pmod{2y}$

が得られる．$D=x_n(F)$，　$E=y_n(F)$ とおくと iii が満たされる．$(\mathrm{mod}\ 2y)$ で考えると $E=y_n(F)\equiv y_n(1)=n$ と補題6から vii を満たす e が存在する．$(\mathrm{mod}\ b)$ で考えると $F\equiv a$ から $D=x_n(F)\equiv x_n(a)=x$，よって補題6から vi を満たす d が存在する．よって i–viii を満たす b, c, d, e, g, x が存在する．

系　整係数の多項式 $f_1(y, n, a, b, c, d, e, g, x)$ が存在し，$1<a$ のとき $y=y_n(a) \Longleftrightarrow f_1(y, n, a, b, c, d, e, g, x)=0$ となる自然数 b, c, d, e, g, x が存在する．

証明　
$$\begin{aligned}f_1(y, n, a, b, c, d, e, g, x) &= \{x^2-(a^2-1)y^2-1\}^2+\{b^2-(a^2-1)(2cy^2)^2-1\}^2\\ &\quad +\{(x+bd)^2-((a+b^2(b^2-a))^2-1)(n+2(e-1)y)^2-1\}^2\\ &\quad +(y-n-g+1)^2\end{aligned}$$
とおけばよい．この式はたしかに整係数の多項式であり，変数は $y, n, a, b, c, d, e, g, x$ である．もし $y=y_n(a)$ ならば，定理27の i, ii, iii, iv を満たす b, c, d, e, g, x が存在するので $f_1(y, n, a, b, c, d, e, g, x)=0$ となる．逆に $f_1(y, n, a, b, c, d, e, g, x)=0$ ならば i, ii, iii, iv が成立し，よって定理27から $y=y_n(a)$ となる．——

$y_n(a)$ は a の $n-1$ 次の多項式であるから，この系はあたりまえだ，と思ってはいけない．この系の意外な点は，n が多項式 f_1 の変数として現われていることである．

§4　指数関係を表わす多項式

この節では $w=z^n$ という関係を w, z, n を変数とする多項式で記述することを目的とする．まずいくつかの不等式と合同式を用意しよう．

補題12　$$1+x \leqq 2^x.$$

証明　$$2^x=(1+1)^x=\sum_{i=0}^{x}\binom{x}{i}=1+x+\cdots\geqq 1+x.$$

補題 13　$$F(x,y)=((x+2)^2-1)((x+1)y)^2+1$$

とおく．もし $F(x,y)=z^2$ となる自然数 z が存在するならば，$x^x<y$．また任意の自然数 x に対して $F(x,y)=z^2$ となる自然数 y,z が存在する．

証明　もし $F(x,y)=z^2$ ならば

$$z^2-((x+2)^2-1)((x+1)y)^2=1$$

から $(x+1)y=y_q(x+2)$ となる自然数 q が存在する．$(\bmod\ x+1)$ で考えると $0\equiv y_q(x+2)\equiv y_q(1)=q$ から $q\geqq x+1$ となる．よって

$$(x+1)y=y_q(x+2)\geqq y_{x+1}(x+2).$$

補題 3 から

$$\geqq(2(x+2)-1)^x>(2x+2)^x=2^x\cdot(x+1)^x.$$

補題 12 から

$$\geqq(x+1)(x+1)^x>(x+1)x^x.$$

よって両辺を $x+1$ で割り $y>x^x$ が得られた．また $((x+2)^2-1)(x+1)^2$ は平方数でないので

$$z^2-((x+2)^2-1)(x+1)^2y^2=1$$

は自然数解 y,z を持つ．このとき式の形から $F(x,y)=z^2$ である．

補題 14　$$z<a\Longrightarrow a\leqq 2az-z^2-1.$$

証明　$f(z)=z^2-2az+a+1$ とおけば $f(1)=1-2a+a+1=2-a\leqq 0$ となり，また $f(z)=(z-a)^2-a^2+a+1$ であるから $z<a$ では単調減少である．よって $1\leqq z<a$ では $f(z)\leqq 0$，つまり $a\leqq 2az-z^2-1$ となる．

補題 15　$z<a$ のとき

$$x_n(a)\equiv z^n+(a-z)y_n(a)\pmod{2az-z^2-1}$$
$$x_n(a)\geqq z^n+(a-z)y_n(a).$$

証明　$f(n)=x_n(a)-z^n-(a-z)y_n(a)$ とおくと

$$\begin{aligned} f(1) &= x_1-z-(a-z)y_1 \\ &= a-z-(a-z) = 0 \\ f(2) &= x_2-z^2-(a-z)y_2 \\ &= (2a^2-1)-z^2-(a-z)\cdot 2a \\ &= 2az-z^2-1. \end{aligned}$$

よって $f(1)\equiv 0$, $f(2)\equiv 0 \pmod{2az-z^2-1}$ となる．$z<a$ と補題 14 から $2az-z^2-1\geqq a>0$ となるので $f(2)>f(1)=0$ となる．よって数学的帰納法を使い $f(n)\equiv f(n+1)\equiv 0$ および $f(n+1)>f(n)$ を示せば十分である．$n=1$ のときは正しいので，n までよいとする．

$$\begin{aligned} f(n+2) &= x_{n+2}-z^{n+2}-(a-z)y_{n+2} \\ &= (2ax_{n+1}-x_n)-z^{n+2}-(a-z)(2ay_{n+1}-y_n) \qquad (\text{補題 } 2) \\ &= 2a(x_{n+1}-z^{n+1}-(a-z)y_{n+1})+2az^{n+1} \\ &\quad -(x_n-z^n-(a-z)y_n)-z^n-z^{n+2} \\ &= 2af(n+1)-f(n)+z^n(2az-z^2-1) \\ &\equiv 0 \pmod{2az-z^2-1} \end{aligned}$$

となる．また不等式に関しては

$$\begin{aligned} &> 2af(n+1)-f(n) \\ &> f(n+1)+f(n+1)-f(n) > f(n+1). \end{aligned}$$

定理 28　$z^n<a$, $w<a$ のとき

$$w = z^n \Longleftrightarrow x_n(a) = w+(a-z)y_n(a)+(i-1)(2az-z^2-1)$$

となる自然数 i が存在する．

証明　$w=z^n$ のとき補題 15 から

$$x_n(a) \equiv w+(a-z)y_n(a) \pmod{2az-z^2-1}$$

となる．$z\leqq z^n<a$ であるから補題 15 から 左辺≧右辺 となり

$$x_n(a) = w+(a-z)y_n(a)+(i-1)(2az-z^2-1)$$

となる自然数 i が存在する．逆に，このような i が存在するとき

$$x_n(a) \equiv w+(a-z)y_n(a) \pmod{2az-z^2-1}.$$

よって補題 15 から $w \equiv z^n \pmod{2az-z^2-1}$ となる．ところが補題 14 から $a \leqq 2az-z^2-1$ であるから $0<w<a \leqq 2az-z^2-1$，$0<z^n<a \leqq 2az-z^2-1$ となり $w=z^n$ が得られる．——

定理 28′　$z^{n+1}<a$，$w<a$ のとき

$$w = z^{n+1} \Longleftrightarrow z\cdot x_n(a) = w+z(a-z)y_n(a)+(i-1)(2az-z^2-1)$$

となる i が存在する．

証明　補題 15 の両辺を z 倍して

$$z\cdot x_n(a) \equiv z^{n+1}+z(a-z)\cdot y_n(a) \pmod{2az-z^2-1}$$

$$z\cdot x_n(a) \geqq z^{n+1}+z(a-z)\cdot y_n(a)$$

に注意すれば，定理 28 の証明と同様に出来る．

系　整係数の多項式 $f_2(w, z, n, a, b, c, d, e, g, h, i, x, y)$ が存在し，$w=z^n \Longleftrightarrow f_2(w, z, n, a, b, c, d, e, g, h, i, x, y)=0$ となる自然数 $a, b, c, d, e, g, h, i, x, y$ が存在する．

証明　$f_2(w, z, n, a, b, c, d, e, g, h, i, x, y)$

$$= f_1{}^2(y, n, a, b, c, d, e, g, x)+\{F(wzn, a)-h^2\}^2$$
$$+\{x-w-(a-z)y-(i-1)(2az-z^2-1)\}^2$$

とおけばよい．f_1 は定理 27 の系の多項式であり，F は補題 13 の多項式である．$w=z^n$ が成り立つとする．補題 13 から $F(wzn, a)=h^2$ となる a, h が存在する．このとき $a>(wzn)^{wzn} \geqq 1$ である．$y=y_n(a)$ とおけば定理 27 から $f_1(y, n, a, b, c, d, e, g, x)=0$ となる b, c, d, e, g, x が存在する．このとき $x=x_n(a)$ である．よって定理 28 から

$$x = w+(a-z)y+(i-1)(2az-z^2-1)$$

となる i が存在する．このとき $f_2(w, z, n, a, b, c, d, e, g, h, i, x, y)=0$ となる．逆に $f_2(w, z, n, a, b, c, d, e, g, h, i, x, y)=0$ のとき，式の形から

(1)　$$f_1(y, n, a, b, c, d, e, g, x) = 0$$

(2)　$F(wzn, a) = h^2$

(3)　$x = w+(a-z)y+(i-1)(2az-z^2-1)$

が成り立つ．(2)から$(wzn)^{wzn}<a$となる．よって$1\leqq w<a$, $z^n<a$が得られる．(1)と定理27から$y=y_n(a)$となり$x=x_n(a)$ともなる．よって(3)と定理28から$w=z^n$が得られる．——

§5　階乗に関する不等式

階乗$k!$を多項式で表わすためには次の方針で進む．まず，kよりnが十分大きければ2項係数$\binom{n}{k}$は

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n^k}{k!}\left(1-\frac{1}{n}\right)\cdots\left(1-\frac{k-1}{n}\right) \doteqdot \frac{n^k}{k!}$$

となる．2項係数$\binom{n}{k}$を得るには2項定理を利用する．つまり

$$(z+1)^n = 1+\binom{n}{1}z+\cdots+\binom{n}{k}z^k+\binom{n}{k+1}z^{k+1}+\cdots+z^n.$$

よって，nよりzを十分大きくすれば$(z+1)^n$をz^{k+1}で割った余りは$1+\binom{n}{1}z+\cdots+\binom{n}{k}z^k$となり，この値の主要部は$\binom{n}{k}z^k$となる．一般に$a$を$b$で割った余り (remainder) が$r$のとき，つまり$a=bq+r$, $0\leqq r<b$のとき，$r=\mathrm{Rem}\,(a, b)$と書き表わす．すると

$$\begin{aligned} k! &\doteqdot n^k \Big/ \binom{n}{k} \\ &\doteqdot \frac{n^k}{\mathrm{Rem}\,((z+1)^n, z^{k+1})/z^k} \\ &= \frac{n^k \cdot z^k}{\mathrm{Rem}\,((z+1)^n, z^{k+1})}. \end{aligned}$$

以上のことを正確に表現するために，いくつかの不等式を準備しよう．

補題16　$k < n,\ n^k < z \Longrightarrow \sum_{i=0}^{k}\binom{n}{i}z^i < \frac{(n^k+1)z^k}{k!}$.

証明　$k=1$のとき 左辺$=1+nz$, 右辺$=(n+1)z=z+nz$. よって

成立する．$2\leqq k$ のとき帰納法を使うために，その前提条件が満たされているか調べると $j<k$ ならば $j<k<n$, $n^j<n^k<z$. よって帰納法が使える．$k-1$ まで正しいとすると

$$\sum_{i=0}^{k}\binom{n}{i}z^i=\sum_{i=0}^{k-1}\binom{n}{i}z^i+\binom{n}{k}z^k$$
$$<\frac{(n^{k-1}+1)z^{k-1}}{(k-1)!}+z^k\cdot\frac{n(n-1)\cdots(n-k+1)}{k!}$$
$$<\frac{z^k}{k!}\left(\frac{k(n^{k-1}+1)}{z}+n^k\right).$$

$$k(n^{k-1}+1)\leqq(n-1)(n^{k-1}+1)=n^k+n-n^{k-1}-1<n^k<z$$

を使えば，求める不等式を得る．

系 $k<n,\ n^k<z\Longrightarrow \mathrm{Rem}\,((z+1)^n, z^{k+1})=\sum_{i=0}^{k}\binom{n}{i}z^i.$

証明 2項定理から

$$(z+1)^n=\sum_{i=0}^{k}\binom{n}{i}z^i+z^{k+1}\left(\sum_{i=k+1}^{n}\binom{n}{i}\cdot z^{i-k-1}\right).$$

補題16から

$$0<\sum_{i=0}^{k}\binom{n}{i}z^i<\frac{(n^k+1)z^k}{k!}$$
$$\leqq(n^k+1)z^k\leqq z\cdot z^k=z^{k+1}.$$

よって，求める式が得られた．

補題17 実数 α が $0\leqq\alpha\leqq\frac{1}{2}$ ならば $\frac{1}{1-\alpha}\leqq1+2\alpha.$

証明 $(1-\alpha)(1+2\alpha)=1+2\alpha-\alpha-2\alpha^2=1+\alpha(1-2\alpha)\geqq1.$

補題18 $(2k)^{2k}<n,\ z=(n+1)^k$ ならば

$$k!<\frac{z^{k+1}}{\mathrm{Rem}\,((z+1)^n, z^{k+1})}<k!+1.$$

証明 $k<(2k)^{2k}<n,\ n^k<n^k+1\leqq(n+1)^k=z$ から補題16およびその系が使えて

$$k! < \frac{(n^k+1)z^k}{\sum_{i=0}^{k}\binom{n}{i}z^i} \leqq \frac{z\cdot z^k}{\mathrm{Rem}\,((z+1)^n,\, z^{k+1})}$$

が得られる．他方

$$\frac{z^{k+1}}{\sum_{i=0}^{k}\binom{n}{i}z^i} < \frac{(n+1)^k\cdot z^k}{\binom{n}{k}\cdot z^k} = \frac{(n+1)^k}{(n+1-1)(n+1-2)\cdots(n+1-k)/k!}$$

$$= k!\Big/\left\{\left(1-\frac{1}{n+1}\right)\left(1-\frac{2}{n+1}\right)\cdots\left(1-\frac{k}{n+1}\right)\right\}$$

$$< k!\Big/\left(1-\frac{k}{n}\right)^k.$$

$2k<(2k)^{2k}<n$ と補題 17 から

$$< k!\left(1+\frac{2k}{n}\right)^k = k!\left(1+\sum_{i=1}^{k}\binom{k}{i}\left(\frac{2k}{n}\right)^i\right)$$

$$\leqq k!\left(1+\frac{2k}{n}\sum_{i=1}^{k}\binom{k}{i}\right) \qquad \left(\because \quad \frac{2k}{n}<1\right)$$

$$< k!\left(1+\frac{2k}{n}\sum_{i=0}^{k}\binom{k}{i}\right) = k!\left(1+\frac{2k}{n}\cdot 2^k\right)$$

$$\leqq k! + \frac{k^k\cdot 2k\cdot 2^k}{n} = k! + \frac{(2k)^{k+1}}{n}$$

$$\leqq k! + \frac{(2k)^{2k}}{n} < k!+1.$$

定理 29　自然数 u, k に対して $u=k!$ であるための必要十分条件は，次の式を満たす自然数 g, h, i, j, n, v, w, z が存在することである．

(1)　$F(2k, n) = g^2$

(2)　$z = (n+1)^k$

(3)　$v = z^{k+1}$

(4)　$w = (z+1)^n$

(5)　$v = u(i+j)+i$

(6) $$w = vh+i+j.$$

証明 十分条件. もし(1)-(6)を満たす自然数が存在したとする. (5)から$0<i+j\leqq u(i+j)<v$, (6)から$i+j=\mathrm{Rem}\,(w,v)$. (5)から$u(i+j)<v<u(i+j)+i+j$. よって両辺を$i+j$で割り, (3), (4)を用いると

$$u<\frac{z^{k+1}}{\mathrm{Rem}\,((z+1)^n, z^{k+1})}<u+1$$

となる. (1)から$(2k)^{2k}<n$であるから補題18から$u=k!$となる.

必要条件. もし$u=k!$ならば補題13から$F(2k,n)=g^2$となるn, gが存在し, $z=(n+1)^k$, $w=(z+1)^n$, $v=z^{k+1}$とおくと補題18から

$$u<\frac{v}{\mathrm{Rem}\,(w,v)}<u+1$$

となる. この式から$0<v-u\cdot\mathrm{Rem}\,(w,v)<\mathrm{Rem}\,(w,v)$であるから$i=v-u\cdot\mathrm{Rem}\,(w,v)$, $j=\mathrm{Rem}\,(w,v)-i$とおけば$v=u\cdot\mathrm{Rem}\,(w,v)+i=u(i+j)+i$となり, また$k+1<(2k)^{2k}<n$から$v<w$となり$w=vh+\mathrm{Rem}\,(w,v)$となる$h$も定まる. ——

この定理29から$k!$を表わす多項式, すなわち§2の(3), (4)を満たす多項式を作るのは容易である. すなわち定理28の系を使えば$(n+1)^k$, z^{k+1}, $(z+1)^n$等が得られるからである. しかしこのようにすると変数の数が多くなるので, 次節で直接素数を表わす多項式を構成しよう.

§6 素数を表わす多項式

すでに十分準備が出来たので, いよいよ次の定理を証明しよう.

定理30 $k+1$が素数である必要十分条件は, 次の式を満たす自然数$a, b, c, d, e, g, h, i, j, m, n, p, q, r, s, t, u, v, w, x, y, z$が存在することである.

(1)　$x^2-(a^2-1)y^2=1$

(2)　$b^2-(a^2-1)C^2=1$

(3)　$D^2-(F^2-1)E^2=1$

(4)　$G^2-(a^2-1)H^2=1$

(5)　$g^2-((2k+2)^2-1)((2k+1)n)^2=1$

(6)　$m^2-((I+2)^2-1)((I+1)a)^2=1$

(7)　$zG=v+z(a-z)H+(q-1)(2az-z^2-1)$

(8)　$v=(ku+u-1)(i+j)+i$

(9)　$w=vh+i+j$

(10)　$x=w+(a-z-1)y+(r-1)(2a(z+1)-(z+1)^2-1)$

(11)　$y=n+H+p$

ただし C, D, E, F, G, H, I は次のように定義される.

(12)　$C=2cy^2$

(13)　$D=x+bd$

(14)　$E=n+2(e-1)y$

(15)　$F=a+b^2(b^2-a)$

(16)　$G=z+(a-n-1)H+(s-1)(2a(n+1)-(n+1)^2-1)$

(17)　$H=k+(t-1)(a-1)$

(18)　$I=n+v+w+z.$

証明　十分条件. (1)-(18) を満たす自然数があったとする. (5), (6) は補題 13 の多項式を使うと $F(2k, n)=g^2$, $F(I, a)=m^2$ となる. よって (18) から

(19)　$$(2k)^{2k}<n$$

(20)　$$(n+v+w+z)^{n+v+w+z}<a$$

となる. (20) から $1<a$, (17) から $0<H$, よって (1), (2), (3), (11), (12), (13), (14), (15) と定理 27 から $x=x_n(a)$, $y=y_n(a)$ となる. (定理 27 における g は, $g=H+p+1$ とおけばよい.) (20) から $n+1<$

a, よって補題14と(16)から$0<G$となる．(4)から或るk'が存在し，$H=y_{k'}(a)$となる．$H=y_{k'}(a)\equiv y_{k'}(1)=k'\ (\mathrm{mod}\ a-1)$と(17)から$k\equiv k'\ (\mathrm{mod}\ a-1)$となる．(11)から$H<y$, よって$k'<n$. (19)から$k<n$, (20)から$n<a$. よって$k, k'<a-1$となり$k=k'$となる．つまり$G=x_k(a)$, $H=y_k(a)$となる．$k<n$と(20)から$(n+1)^k<(n+1)^n<a$, $z<a$. 定理28と(16)から$z=(n+1)^k$. (20)から$(z+1)^n<a$, $w<a$. 定理28と(10)から$w=(z+1)^n$. (20)から$z^{k+1}\leqq z^n<a$, $v<a$. 定理28′と(7)から$v=z^{k+1}$. よって(8), (9)と定理29から$ku+u-1=k!$, つまり$(k+1)u=k!+1$. これはウィルソンの定理から$k+1=$素数を意味する．

必要条件．$k+1$が素数とする．まず$(k+1)u=k!+1$となる自然数uが定まる．つまり$ku+u-1=k!$となる．定理29から(5), (8), (9)を満たすg, h, i, j, n, v, w, zが存在し，$z=(n+1)^k$, $v=z^{k+1}$, $w=(z+1)^n$となる．$I=n+v+w+z$とおき$F(I, a)=m^2$となるa, mを定める．このとき(19), (20)が成立し，特に$1<a$. また$y=y_n(a)$とおくと定理27から(1), (2), (3), (12), (13), (14), (15)を満たすb, c, d, e, xが存在し，$x=x_n(a)$となる．$G=x_k(a)$, $H=y_k(a)$とおくと(4)が満たされ，補題4から

$$n+H=n+y_k(a)\leqq n+y_{n-1}(a)<y_n(a).$$

よって(11)を満たすpが定まる．(19), (20)から$(n+1)^k<a$, $z<a$, $(z+1)^n<a$, $w<a$, $z^{k+1}<a$, $v<a$が得られるので定理28, 28′から(7), (10), (16)を満たすq, r, sが定まる．$H=y_k(a)\equiv y_k(1)=k\ (\mathrm{mod}\ a-1)$から(17)を満たす$t$も定まる．——

さて，(8), (9), (10), (11)の式の形からv, w, x, yを消去出来る．よってこの章の目的であった次の定理を得る．

定理 31 次の19変数の多項式は素数を表わす多項式である．

$f(a, b, c, d, e, g, h, i, j, k, m, n, p, q, r, s, t, u, z)$

$$= (k+1)[1-\{X^2-(a^2-1)Y^2-1\}^2-\{b^2-(a^2-1)C^2-1\}^2$$
$$-\{D^2-(F^2-1)E^2-1\}^2-\{G^2-(a^2-1)H^2-1\}^2$$
$$-\{g^2-((2k+2)^2-1)((2k+1)n)^2-1\}^2$$
$$-\{m^2-((I+2)^2-1)((I+1)a)^2-1\}^2$$
$$-\{zG-V-z(a-z)H-(q-1)(2az-z^2-1)\}^2]$$

ただし $C, D, E, F, G, H, I, V, W, X, Y$ は次のように定義される.

$$V = (ku+u-1)(i+j)+i$$
$$W = Vh+i+j$$
$$H = k+(t-1)(a-1)$$
$$G = z+(a-n-1)H+(s-1)(2a(n+1)-(n+1)^2-1)$$
$$Y = n+H+p$$
$$X = W+(a-z-1)Y+(r-1)(2a(z+1)-(z+1)^2-1)$$
$$C = 2cY^2$$
$$D = X+bd$$
$$E = n+2(e-1)Y$$
$$F = a+b^2(b^2-a)$$
$$I = n+V+W+z.$$

証明　式の形から V, H, F が定まり，V から W, V と W から I, H から G と Y, W と Y から X, Y から C と E, X から D が定まるので，定理の式は確かに 19 変数の多項式である．変数に自然数の値を代入したとき，V は正，よって W も正，H は正，よって Y も正となる．すなわち定理 30 を利用するとき，X が正であることを確かめさえすればよい．証明は§2 で説明した Putnum の技法を用いればよい．

まず $f(a, b, \cdots, z)>0$ とすると，定理 30 の(1)-(7)の v, x, y を大文字に変えた式が成立する．よって(20)の v, w を V, W に変えた式も成り立つ．この式から $z+1<a$ が成り立つので $X>0$ となる．

V, W, X, Y が正であるから $v=V, w=W, x=X, y=Y$ とおけば，定理30の(1)-(18)が成立する．よって $k+1=$ 素数 となり $f(a, b, \cdots, z)=(k+1)(1-0)=k+1=$ 素数 となる．逆に p が素数のとき，$p=k+1$ とおくと定理30の(1)-(18)が成り立つ．よって $V=v, W=w, X=x, Y=y$ となり

$$f(a, b, \cdots, z) = (k+1)(1-0) = k+1 = p$$

となる．——

§7 残された問題

定理31において得られた多項式は，19変数の37次式である．なぜならば定理31において V は3次，W は4次，I は4次．よって定理30において(6)は18次式となり，定理31において自乗して $k+1$ を掛けると37次式となり，他の項もすべて計算してみると37次より小さくなるからである．

変数を多くすれば，次数は5次まで下げられる．なぜならば定理30において3次以上の項が現われたならば，それらは x^2, xy という形に何か掛けたものである．よって新しい変数 z_1, z_2 を導入し

$$x^2 = z_1$$

$$xy = z_2$$

という関係式をつけ加え，x^2 のところを z_1 に，xy のところを z_2 におきかえれば次数が1つ下がる．この操作をくり返すと，すべての式が2次以下となる．これらの式の左辺から右辺を引き，自乗し，加え合わせ，1から引き，$k+1$ を掛けると，定理31の式が得られるのだから5次式となる．たとえば(5)は

$$(2k+2)^2 = z_1$$

$$(2k+1)n = z_2$$

$$z_2{}^2 = z_3$$

とおくと

$$g^2-(z_1-1)z_3=1$$

となり，定理 31 においては，f は

$$(k+1)[1-\cdots-\{(2k+2)^2-z_1\}^2-\{(2k+1)n-z_2\}^2-\{z_2{}^2-z_3\}^2$$
$$-\{g^2-(z_1-1)z_3-1\}^2\cdots]$$

と変わるわけである．5 次より下げられるか否かは未解決である．

次に変数の数について考えよう．Matijasevič[3] が最初に作った式は 24 変数であった．次に Matijasevič–Robinson[4] が一般論から 14 変数の式を作った．次に著者[7]が一般論を素数を表わす式に作り変えて 12 変数の式を作った．次に Matijasevič[5] が 10 変数の式を作った．この 10 変数の式は次数が大きく，11281 次である．もっと変数の数を下げられるだろうけれど，1 変数では出来ない．つまり

定理 32　素数を表わす多項式は 2 変数以上必要である．

証明　もし 1 変数で得られたとして

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n \qquad (a_i=\text{整数})$$

が素数を表わす多項式だったと仮定する．つまり

(1) x を自然数だとしたとき，$f(x)>0$ ならば $f(x)$ は素数である．

(2) どのような素数 p も適当に自然数 x を選ぶと $p=f(x)$ となる．

このとき (2) から $f(x)$ は無限に多くの正の値をとらねばならないから $a_0>0$ でなければならない．なぜなら $a_0<0$ とすると

$$x>M=|a_1|+|a_2|+\cdots+|a_n|$$

のとき

$$\begin{aligned}&a_1x^{n-1}+\cdots+a_n\\&\quad\leqq|a_1x^{n-1}+\cdots+a_n|\\&\quad\leqq|a_1|x^{n-1}+\cdots+|a_n|\\&\quad\leqq|a_1|x^{n-1}+\cdots+|a_n|x^{n-1}\end{aligned}$$

$$= (|a_1|+\cdots+|a_n|)x^{n-1}$$
$$< x^n \leqq -a_0x^n.$$

よって $f(x)<0$ となってしまい，$f(x)$ は $1\leqq x\leqq M$ の間の有限個の自然数に対してのみ正になる可能性しかないからである．

$a_0>0$ ならば $x>M$ のとき，同じ計算により

$$f(x) \geqq a_0x^n-|a_1x^{n-1}+\cdots+a_n| > 0$$

となる．また $f(x)$ を微分すると

$$f'(x) = na_0x^{n-1}+(n-1)a_1x^{n-2}+\cdots+a_{n-1}$$

となる．$na_0>0$ であるので

$$x > N = (n-1)|a_1|+(n-2)|a_2|+\cdots+|a_{n-1}|$$

のときは $f'(x)>0$ つまり $f(x)$ は単調増大である．よって M と N の大きい方を L とおくと

$$x > L \Longrightarrow f(x) > 0,\ \ f(x+1) > f(x)$$

となる．よって $m>L$ ならば(1)から $f(m)=p=$素数 でなければならず，$n=m+p$ とおくと $f(n)>f(m)=p$ であり，しかも

$$f(n) = f(m+p) \equiv f(m) = p \equiv 0 \pmod p$$

となる．つまり $f(n)$ は p より大きく，p で割り切れる．これは $f(n)$ は素数でないことを意味する．(1)から $f(n)$ は素数でなければならないから矛盾である．つまり，1変数で素数を表わす式は作れない．
——

では，2変数では可能であろうか．おそらく不可能であろうと予想されるが，その証明は出来ていない．また10変数より少しずつ下げていき，どこまで行きつくか未解決な問題である．

もし，さらに興味ある人はまず Davis[1] を読み，素数を表わす多項式とヒルベルトの第10問題との関係を学ぶとよい．次に Matijasevič–Robinson[4] の Part 1 を読み，次に Jones–Sato–Wada–Wiens[2] を読むと，12変数で可能なことがわかる．Matijasevič

[5]は手に入りにくいが，英訳されたものがそのうち公表されると思う．

[1]　Martin Davis, Hilbelt's tenth problem is unsolvable, Amer. Math. Monthly, 80(1973), 233-269.

[2]　J. Jones, D. Sato, H. Wada & D. Wiens, Diophantine representation of the set of prime numbers, Amer. Math. Monthly, 83(1976), 449-464.

[3]　Yuri Matijasevič, Diophantine representation of the set of prime numbers, Doklady Akademii Nauk SSSR, 196(1971), 770-773.

[4]　Yuri Matijasevič & Julia Robinson, Reduction of an arbitrary Diophantine equation to one in 13 unknowns, Acta Arithmetica, 27 (1975), 521-553.

[5]　Yuri Matijasevič, Primes are non-negative values of a polynomial in 10 variables, Nauk, Leningrad, 1977.

[6]　Hilary Putnam, An unsolvable problem in number theory, Journal of Symbolic Logic, 25(1960), 220-232.

[7]　和田秀男，素数を表わす多項式について，数学，27(1975), 160-161.

参考書案内

この本を書くために参考にした本を並べてみよう．

(1)　稲葉栄次著，整数論，共立出版

(2)　I. M. ヴィノグラドフ著(三瓶与右衛門，山中健訳)，整数論入門，共立出版

(3)　O. オア著(本田欣哉訳)，整数論，河出書房

(4)　銀林浩著，初等整数論入門，国土社

(5)　草場公邦著，整数論，日本放送出版協会

(6)　高木貞治著，初等整数論講義，共立出版

これらのうち，(3)は非常にやさしい本で，中学生でも読めると思う．(2)は教科書のように少ない分量の中に，要領よくびっしりとまとまっている．(6)は内容が豊富であり，名著である．さらに高度な本としては

(7)　ボレビッチ，シャハレビッチ著(佐々木義雄訳)，整数論，吉岡書店

(8)　高木貞治著，代数的整数論，岩波書店

などがある．

p	r	p	r	p	r	p	r	p	r	p	r
1 091	2	1 303	7	1 549	2	1 777	5	2 017	5	2 269	2
1 093	5	1 307	2	1 553	3	1 783	11	2 027	2	2 273	3
1 097	3	1 319	13	1 559	19	1 787	2	2 029	2	2 281	7
1 103	5	1 321	13	1 567	3	1 789	19	2 039	7	2 287	19
1 109	2	1 327	3	1 571	2	1 801	11	2 053	2	2 293	2
1 117	2	1 361	3	1 579	3	1 811	41	2 063	5	2 297	5
1 123	2	1 367	5	1 583	5	1 823	5	2 069	2	2 309	2
1 129	11	1 373	2	1 597	11	1 831	3	2 081	3	2 311	3
1 151	17	1 381	2	1 601	3	1 847	5	2 083	2	2 333	2
1 153	5	1 399	13	1 607	5	1 861	2	2 087	5	2 339	2
1 163	5	1 409	3	1 609	7	1 867	2	2 089	7	2 341	7
1 171	2	1 423	3	1 613	3	1 871	19	2 099	2	2 347	3
1 181	7	1 427	2	1 619	2	1 873	37	2 111	7	2 351	13
1 187	2	1 429	11	1 621	2	1 877	2	2 113	5	2 357	2
1 193	3	1 433	3	1 627	3	1 879	11	2 129	3	2 371	2
1 201	11	1 439	7	1 637	2	1 889	3	2 131	2	2 377	5
1 213	2	1 447	3	1 657	11	1 901	2	2 137	23	2 381	3
1 217	3	1 451	2	1 663	3	1 907	2	2 141	2	2 383	5
1 223	5	1 453	2	1 667	2	1 913	3	2 143	3	2 389	2
1 229	2	1 459	3	1 669	2	1 931	2	2 153	3	2 393	3
1 231	3	1 471	7	1 693	2	1 933	5	2 161	23	2 399	11
1 237	2	1 481	3	1 697	3	1 949	2	2 179	7	2 411	17
1 249	7	1 483	2	1 699	3	1 951	3	2 203	5	2 417	3
1 259	2	1 487	5	1 709	3	1 973	2	2 207	5	2 423	5
1 277	2	1 489	29	1 721	3	1 979	2	2 213	2	2 437	2
1 279	3	1 493	2	1 723	3	1 987	2	2 221	2	2 441	11
1 283	2	1 499	2	1 733	2	1 993	5	2 237	2	2 447	5
1 289	11	1 511	11	1 741	2	1 997	2	2 239	3	2 459	2
1 291	2	1 523	2	1 747	2	1 999	3	2 243	2	2 467	2
1 297	17	1 531	2	1 753	7	2 003	5	2 251	7	2 473	5
1 301	2	1 543	5	1 759	7	2 011	3	2 267	2	2 477	2

p	r	p	r	p	r	p	r	p	r	p	r
4 013	2	4 261	2	4 547	2	4 801	7	5 077	2	5 381	3
4 019	2	4 271	7	4 549	7	4 813	2	5 081	3	5 387	2
4 021	2	4 273	5	4 561	11	4 817	3	5 087	5	5 393	3
4 027	3	4 283	2	4 567	3	4 831	3	5 099	2	5 399	7
4 049	3	4 289	3	4 583	5	4 861	11	5 101	11	5 407	3
4 051	17	4 297	5	4 591	11	4 871	11	5 107	2	5 413	5
4 057	5	4 327	3	4 597	5	4 877	2	5 113	19	5 417	3
4 073	3	4 337	3	4 603	2	4 889	3	5 119	3	5 419	3
4 079	11	4 339	11	4 621	2	4 903	3	5 147	2	5 431	3
4 091	2	4 349	2	4 637	2	4 909	13	5 153	5	5 437	5
4 093	2	4 357	2	4 639	3	4 919	13	5 167	13	5 441	3
4 099	2	4 363	2	4 643	5	4 931	11	5 171	2	5 443	2
4 111	17	4 373	2	4 649	3	4 933	2	5 179	2	5 449	7
4 127	5	4 391	17	4 651	3	4 937	3	5 189	2	5 471	7
4 129	13	4 397	2	4 657	23	4 943	7	5 197	7	5 477	2
4 133	2	4 409	3	4 663	3	4 951	7	5 209	17	5 479	3
4 139	2	4 421	3	4 673	3	4 957	2	5 227	2	5 483	2
4 153	5	4 423	3	4 679	11	4 967	5	5 231	7	5 501	2
4 157	2	4 441	43	4 691	2	4 969	11	5 233	13	5 503	3
4 159	3	4 447	3	4 703	5	4 973	2	5 237	3	5 507	2
4 177	5	4 451	2	4 721	7	4 987	2	5 261	2	5 519	13
4 201	11	4 457	3	4 723	2	4 993	5	5 273	3	5 521	11
4 211	7	4 463	5	4 729	17	4 999	3	5 279	7	5 527	5
4 217	3	4 481	3	4 733	5	5 003	2	5 281	7	5 531	13
4 219	2	4 483	2	4 751	19	5 009	3	5 297	3	5 557	2
4 229	2	4 493	2	4 759	3	5 011	2	5 303	5	5 563	2
4 231	3	4 507	2	4 783	11	5 021	3	5 309	2	5 569	13
4 241	3	4 513	7	4 787	2	5 023	3	5 323	5	5 573	2
4 243	2	4 517	2	4 789	2	5 039	11	5 333	2	5 581	19
4 253	2	4 519	3	4 793	3	5 051	2	5 347	3	5 591	11
4 259	2	4 523	5	4 799	7	5 059	2	5 351	11	5 623	5

p	r	p	r	p	r	p	r	p	r	p	r
7 243	2	7 547	2	7 817	3	8 101	29	8 387	2	8 681	29
7 247	5	7 549	2	7 823	5	8 111	11	8 389	19	8 689	13
7 253	2	7 559	13	7 829	2	8 117	2	8 419	3	8 693	2
7 283	2	7 561	13	7 841	13	8 123	2	8 423	5	8 699	2
7 297	5	7 573	2	7 853	2	8 147	2	8 429	2	8 707	5
7 307	2	7 577	3	7 867	3	8 161	7	8 431	3	8 713	5
7 309	19	7 583	5	7 873	5	8 167	3	8 443	2	8 719	3
7 321	7	7 589	2	7 877	2	8 171	2	8 447	5	8 731	2
7 331	2	7 591	37	7 879	3	8 179	2	8 461	23	8 737	5
7 333	19	7 603	2	7 883	2	8 191	17	8 467	2	8 741	2
7 349	2	7 607	5	7 901	2	8 209	7	8 501	7	8 747	2
7 351	7	7 621	2	7 907	2	8 219	2	3 513	5	8 753	3
7 369	7	7 639	7	7 919	7	8 221	2	8 521	13	8 761	23
7 393	5	7 643	2	7 927	3	8 231	11	8 527	5	8 779	11
7 411	2	7 649	3	7 933	2	8 233	37	8 537	3	8 783	5
7 417	5	7 669	2	7 937	3	8 237	2	8 539	2	8 803	2
7 433	3	7 673	3	7 949	2	8 243	2	8 543	5	8 807	5
7 451	2	7 681	17	7 951	13	8 263	3	8 563	2	8 819	2
7 457	3	7 687	11	7 963	5	8 269	2	8 573	2	8 821	2
7 459	2	7 691	2	7 993	5	8 273	3	8 581	7	8 831	7
7 477	2	7 699	3	8 009	3	8 287	3	8 597	2	8 837	2
7 481	7	7 703	5	8 011	43	8 291	2	8 599	3	8 839	3
7 487	5	7 717	2	8 017	5	8 293	2	8 609	3	8 849	3
7 489	7	7 723	3	8 039	11	8 297	3	8 623	3	8 861	2
7 499	2	7 727	5	8 053	2	8 311	3	8 627	2	8 863	3
7 507	2	7 741	7	8 059	3	8 317	19	8 629	17	8 867	2
7 517	2	7 753	31	8 069	2	8 329	7	8 641	17	8 887	3
7 523	2	7 757	2	8 081	3	8 353	5	8 647	3	8 893	5
7 529	3	7 759	3	8 087	5	8 363	2	8 663	5	8 923	2
7 537	7	7 789	2	8 089	17	8 369	3	8 669	2	8 929	11
7 541	2	7 793	3	8 093	2	8 377	5	8 677	2	8 933	2

最小原始根(≠素数)の表

p	r	p	r	p	r	p	r	p	r	p	r
41	6	1 297	10	3 001	14	4 549	6	6 337	10	8 011	14
109	6	1 303	6	3 061	6	4 657	15	6 421	6	8 101	6
151	6	1 429	6	3 079	6	4 721	6	6 521	6	8 233	10
229	6	1 471	6	3 109	6	4 783	6	6 553	10	8 317	6
251	6	1 489	14	3 221	10	4 909	6	6 581	14	8 389	6
271	6	1 759	6	3 229	6	4 931	6	6 661	6	8 461	6
313	10	1 783	10	3 251	6	4 951	6	6 793	10	8 581	6
337	10	1 789	6	3 301	6	5 101	6	6 841	22	8 629	6
367	6	1 811	6	3 313	10	5 167	6	6 991	6	8 681	15
409	21	1 871	14	3 319	6	5 233	10	7 177	10	8 941	6
439	15	1 873	10	3 361	22	5 531	10	7 309	6	9 103	6
733	6	1 879	6	3 631	15	5 581	6	7 333	6	9 109	10
761	6	2 137	10	3 967	6	5 641	14	7 351	6	9 133	6
971	6	2 411	6	4 051	10	5 743	10	7 481	6	9 157	6
991	6	2 441	6	4 111	12	5 791	6	7 591	6	9 439	22
1 021	10	2 551	6	4 211	6	5 821	6	7 687	6	9 697	10
1 031	14	2 749	6	4 339	10	5 839	6	7 753	10	9 781	6
1 069	6	2 791	6	4 391	14	6 073	10	7 841	12	9 829	10
1 289	6	2 971	10	4 441	21	6 301	10	7 951	6	9 931	10

索　　引

あ　行

か　行

さ　行

た　行

数の世界—整数論への道

1981年7月10日　第1刷発行 ©

定価 2200 円

著　者　和田秀男（わだ ひでお）

発行者　緑川　亨

〒101　東京都千代田区一ツ橋 2-5-5
発行所　株式会社 岩波書店
電話 03-265-4111
振替 東京 6-26240

印刷・理想社　製本・田中製本